

John R. Parker, Jr., California Bar No. 257761
ALMEIDA LAW GROUP LLC
3550 Watt Avenue, Suite 140
Sacramento, California 95821
jrparker@almeidalawgroup.com

David S. Almeida (*pro hac vice forthcoming*)
Britany Kabakov (*pro hac vice forthcoming*)
Matthew J. Langley, California Bar No. 342846
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
t: 312-576-3024
david@almeidalawgroup.com
matt@almeidalawgroup.com
britany@almeidalawgroup.com

Attorneys for Plaintiffs & the Proposed Class

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

L.V., S.T. and C.R.T., individually and on behalf of all others similarly situated,

Case No.: 2:23-cv-09658

Plaintiffs.

VS.

ALTAMED HEALTH SERVICES CORP.,

Defendant.

CLASS ACTION COMPLAINT

1. VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE SECTION 56, *et seq.*
 2. VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE SECTION 630, *et seq.*
 3. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE SECTION 17200, *et seq.*
 4. INVASION OF PRIVACY - INTRUSION UPON SECLUSION

5. BREACH OF IMPLIED CONTRACT
 6. VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, CAL. CIV. CODE SECTION 1750, *et seq.*
 7. NEGLIGENCE
 8. BREACH OF CONFIDENCE
 9. BREACH OF FIDUCIARY DUTY
 10. UNJUST ENRICHMENT
 11. VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. SECTION 2511(1), *et seq.*

DEMAND FOR JURY TRIAL

1 Plaintiffs L.V., S.T. and C.R.T. (collectively, “**Plaintiffs**”), individually and on
 2 behalf of all others similarly situated, bring this action against Defendant AltaMed
 3 Health Service Corporation (“**AltaMed**” and/or “**Defendant**”). Plaintiffs’ allegations
 4 are based upon personal knowledge as to themselves and their own acts, and upon
 5 information and good faith belief as to all other matters based on the investigation
 6 conducted by Plaintiffs’ attorneys.

7 **INTRODUCTION**

8 1. This case concerns a very serious breach of Defendant’s data privacy
 9 and security obligations as it installed certain tracking technologies on its digital
 10 properties to collect and disclose to unauthorized third parties Plaintiffs’ and Class
 11 Members’ personally identifiable information (“**PII**”) and protected health
 12 information (“**PHI**”) (collectively referred to as “**PII/PHI**” or “**Private
 13 Information**”) for its own pecuniary gain.

14 2. Information concerning a person’s physical and mental health is among
 15 the most confidential and sensitive information in our society, and the mishandling
 16 of such information can have serious consequences including, but certainly not
 17 limited to, discrimination in the workplace and/or denial of insurance coverage.¹

18 3. Simply put, if people do not trust that their sensitive private information
 19 will be kept private and secure, they may be less likely to seek medical treatment,
 20 which can lead to much more serious health consequences down the road. In
 21 addition, protecting medical information and making sure it is kept confidential and

22
 23
 24 ¹ See Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New*
research found pervasive use of tracking tech on substance-abuse-focused health
care websites, potentially endangering users in a post-Roe world, WIRED (Nov. 16,
 25 2022), available at <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited Nov. 10, 2023) (“While the sharing of any kind
 26 of patient information is often strictly regulated or outright forbidden, it’s even more
 27 verboten in addiction treatment, as patients’ medical history can be inherently
 28 criminal and stigmatized.”).

1 not disclosed to unauthorized entities is vitally necessary to maintain public trust in
 2 the healthcare system as a whole.

3 4. Reiterating the importance of and necessity for data security and privacy
 4 concerning health information, the Federal Trade Commission (“FTC”) recently
 5 published a bulletin entitled *Protecting the privacy of health information: A Baker’s*
6 dozen takeaways from FTC cases, in which it noted that “[h]ealth information is not
 7 just about medications, procedures, and diagnoses. **Rather, it is anything that**
8 conveys information—or enables an inference—about a consumer’s health.
 9 Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx*
 10 and *Flo Health* **make clear that the fact that a consumer is using a particular**
 11 **health-related app or website—one related to mental health or fertility, for**
 12 **example—or how they interact with that app (say, turning ‘pregnancy mode’ on**
 13 **or off) may itself be health information.”²**

14 5. The FTC is unequivocal in its stance as it informs—in no uncertain
 15 terms—healthcare companies that they should **not** use tracking technologies to
 16 collect sensitive health information and disclose it to various platforms without
 17 informed consent:

18 ***Don’t use behind-the-scenes tracking technologies that***
 19 ***contradict your privacy promises or otherwise harm***
 20 ***consumers.***

21 In today’s surveillance economy, the consumer is often the
 22 product. Consumer data powers the advertising machine that
 23 goes right back to the consumer. **But when companies use**
 24 **consumers’ sensitive health data for marketing and**
advertising purposes, such as by sending that data to

25 ² See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen*
 26 *takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis
 27 added), available at <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases> (last visited Nov. 10, 2023).

1 **marketing firms via tracking pixels on websites or software**
2 **development kits on apps, watch out.**

3 [Recent FTC enforcement actions such as]
4 *BetterHelp, GoodRx, Premom, and Flo* make clear that
5 practices like that **may run afoul of the FTC Act if they**
6 **violate privacy promises or if the company fails to get**
7 **consumers' affirmative express consent for the disclosure**
8 **of sensitive health information.**³

9 6. Most recently, in July 2023, federal regulators sent a letter to
10 approximately 130 healthcare providers warning them about the use of online
11 tracking technologies that could result in unauthorized disclosures of Sensitive
12 Information to third parties. The letter highlighted the “risks and concerns about the
13 use of technologies, such as the Meta/Meta Pixel and Google Analytics, that can
14 track a user’s online activities,” and warned about “[i]mpermissible disclosures of
15 an individual’s personal health information to third parties” that could “result in a
16 wide range of harms to an individual or others.” According to the letter, “[s]uch
17 disclosures can reveal sensitive information including health conditions, diagnoses,
18 medications, medical treatments, frequency of visits to health care professionals,
19 where an individual seeks medical treatment, and more.”⁴

20 7. Despite these warnings from federal regulators, Defendant deployed
21 tracking technologies that allowed third-party companies, such as Facebook, to
22 intercept the Private Information of visitors to and users of its websites (“**Users**” or
23 “**Class Members**”) to sell targeted advertising and/or otherwise monetize that
24 information in the ever-growing marketplace for PII and PHI.

25

³ *Id.* (emphasis added) (further noting that *GoodRx & Premom* underscore that this
26 conduct may also violate the Health Breach Notification Rule, which requires
27 notification to consumers, the FTC and, in some cases, the media, of disclosures of
28 health information without consumers’ authorization).

⁴ See https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

1 8. Defendant AltaMed is a not-for-profit healthcare system that offers
2 healthcare services, including primary care, urgent care, dental services and HIV
3 services, with locations throughout the greater Los Angeles area.

4 9. Defendant has disregarded the privacy rights of Users by intentionally,
5 willfully, recklessly and/or negligently failing to implement adequate and
6 reasonable measures to ensure that the Users' Private Information was safeguarded.
7 Instead, Defendant made the conscious decision to use certain tracking technologies,
8 which allowed unauthorized third parties, including Meta Platforms, Inc. d/b/a Meta
9 ("Facebook"), to intercept Users' clicks, communications on and visits to
10 Defendant's websites, including <https://www.altamed.org/> (the "Website") and
11 <https://www.myaltamed.net> (the "Portal" and collectively with the website, the
12 "Web Properties").

13 10. AltaMed's "Notice of Privacy Practices" ("Privacy Policy") informs
14 Users that AltaMed "is committed to safeguarding your protected health information"
15 and that "sharing of your PHI for marketing purposes would require your prior written
16 authorization."⁵ AltaMed's Privacy Policy also promises that "AltaMed will only use
17 or share your health information if it is needed to provide you with health services"
18 and that "[i]f AltaMed needs to share your PHI for a reason not explained in this
19 Notice, we will first need your written permission unless required by law" and that
20 "[m]ost uses and sharing of your PHI for marketing purposes would require your prior
21 written authorization."

22 11. Unbeknownst to Users and without their authorization or informed
23 consent, Defendant installed Facebook's tracking tool, the Meta Pixel ("Meta
24 Pixel" or "Pixel") and other third-party tracking technologies, on its Web Properties

25
26

⁵ AltaMed Privacy Policy,
27 https://www.altamed.org/sites/default/files/documents/2023-08/english_proj14075_nopp_update_final_082323-xxs-compressed.pdf (last visited
28 Nov. 10, 2023).

1 in order to intercept and send Private Information to third parties such as Facebook
2 and/or Google LLC.

3 12. The Pixel is a piece of code that Defendant commonly used to track,
4 capture, and disclose activity and experiences on its Web Properties.

5 13. But no mention of Facebook or its Pixel is made in AltaMed's Privacy
6 Policy or Website, and there is no indication that AltaMed will be in the business of
7 transmitting its Users' PHI to third parties via its Website.⁶

8 14. Defendant encouraged Plaintiffs and Class Members to access and use
9 various digital tools via its Web Properties to, among other things, receive
10 healthcare services, in order to gain additional insights into its Users, improve its
11 return on marketing dollars and, ultimately, increase its revenue.

12 15. Plaintiffs and Class Members who visited and used Defendant's Web
13 Properties understandably thought they were communicating with only their trusted
14 healthcare providers, and reasonably believed that their sensitive and private PII and
15 PHI would be guarded with the utmost care. In browsing Defendant's Web
16 Properties—be it to make an appointment, locate a doctor with a specific specialty,
17 find sensitive information about their diagnosis, or investigate treatment for their
18 diagnosis—Plaintiffs and Class Members did not expect that every search (including
19 exact words and phrases they typed into Defendant's website search bars), page visits,
20 or even their access/interactions on Defendant's online portals would be intercepted,
21 captured, or otherwise shared with Facebook in order to target Plaintiffs and Class
22 Members with advertisements, in conscious disregard of their privacy rights.

23 16. In exchange for installing the Pixels, Facebook provides Defendant with
24 analytics about the advertisements it has placed as well as tools to target people who
25 have visited its Web Properties.

26 17. As background, Pixels are snippets of code that track Users as they
27 navigate through a website—logging which pages they visit, each button they click

28⁶ *Id.*

1 and what information they provide in online forms. These Pixels collect Users' 2 confidential and Private Information—including details about their medical 3 conditions, treatments, providers sought and appointments—and send it to Facebook 4 without prior, informed consent.

5 18. More specifically, the Meta Pixel sends information to Facebook via 6 scripts running in a person's internet browser, so each data packet comes labeled 7 with a specific internet protocol ("IP") address that can be used in combination with 8 other data to identify an individual or household. Additionally, if the person has an 9 active Facebook account, the IP address is paired with their personal unique 10 Facebook ID ("FID"), which Facebook uses to identify that individual.⁷

11 19. While the information captured and disclosed without permission may 12 vary depending on the Pixel(s) embedded, these "data packets" can be extensive, 13 transmitting, for example, not just the name of the physician and her field of medicine, 14 but also the first name, last name, email address, phone number, zip code and city of 15 residence entered in the booking form. That data is linked to a specific IP address. 16 The amalgamation of these data points and unique identifying information results in 17 an egregious, unauthorized dissemination of highly sensitive Private Information 18 unique to each individual User.

19 20. The Meta Pixel tracks and log each page a user visits, what buttons they 20 click, as well as specific information they input into a website. In addition, if the 21 person is (or has in the last 365 days) logged into Facebook when they visit a 22 particular website when a Meta Pixel is installed, some browsers will attach third- 23 party cookies—another tracking mechanism—that allow Facebook to link Pixel data 24

25 ⁷ Regardless, Facebook tracks and collects data even on people who don't have a 26 Facebook account or have deactivated their Facebook accounts. They can be in an 27 even worse situation since the data is being collected about them, but because they 28 don't have an account (or an active account), they cannot clear past activity or disconnect the collection of future activity. In the past, these were referenced as "ghost accounts" or "shadow profiles."

1 to specific Facebook accounts.

2 21. Alarmingly, the use of Meta Pixels on Defendant’s Web Properties tracks
3 extremely sensitive PHI such as health conditions (e.g., diabetes or cancer), diagnoses
4 (e.g., COVID-19 or HIV/AIDS), procedures, treatment sought, the treating physician
5 (including their specialty and location) and PII such as unique personal identifiers
6 including but not limited to, the patient’s FID and their IP address.

7 22. In addition to the Meta Pixel, Defendant, upon information and good
8 faith belief, also installed and implemented Facebook’s Conversions Application
9 Programming Interface (“CAPI”) on its Web Properties servers.⁸

10 23. Unlike the Meta Pixel, which co-opts a website user’s browser and
11 forces it to disclose information to third parties in addition to the website owner,
12 CAPI does not cause the User’s browser to transmit information directly to
13 Facebook. Rather, CAPI tracks the User’s website interaction, including Private
14 Information, records and stores that information on the website owner’s servers and
15 then transmits the data to Facebook from the website owner’s servers.⁹

16 24. Indeed, Facebook markets CAPI as a “better measure [of] ad
17 performance and attribution across your customer’s full journey, from discovery to
18 conversion. This helps you better understand how digital advertising impacts both

22 25 26 27 28 ⁸ CAPI “works with your Meta Pixel to help improve the performance and
measurement of your Facebook ad campaigns.” See
<https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited Nov. 8, 2023).

22 23 24 25 26 27 28 ⁹ “Server events are linked to a dataset ID and are processed like events sent via the
Meta Pixel.... This means that server events may be used in measurement,
reporting, or optimization in a similar way as other connection channels,”
<https://revealbot.com/blog/facebook-conversions-api/> (last visited Nov. 8, 2023).

1 online and offline results.”¹⁰

2 25. Despite the clear and unequivocal prohibition on the disclosure of
 3 Private Information, including PHI, without consent, Defendant chose to use the
 4 Pixel and CAPI data for marketing purposes in an effort to bolster its profits.
 5 Defendant put its desire for profit over its patients’ privacy rights.

6 26. Plaintiffs had their Private Information, including sensitive medical
 7 information, harvested by Facebook through the Meta Pixel tracking tool without
 8 their consent when they entered their information into Defendant’s Web Properties,
 9 and continued to have their privacy violated when their Private Information was used
 10 to turn a profit by way of targeted advertising related to their respective medical
 11 conditions and treatments sought.

12 27. Defendant knew that by embedding the Meta Pixel—a proprietary
 13 tracking and advertising tool developed by Facebook—on its Web Properties, it was
 14 permitting Facebook to collect and use Plaintiffs’ and Class Members’ Private
 15 Information, including sensitive medical information.

16 28. Defendant (or any third parties) did not obtain Plaintiffs’ and Class
 17 Members’ prior consent before sharing their sensitive, confidential communications
 18 and Private Information with third parties such as Facebook, the largest social media
 19 company on earth, which has a sordid history of privacy violations in pursuit of
 20 ever-increasing advertising revenue.¹¹

21 29. Defendant failed to issue a notice that Plaintiffs’ and Class Members’

22 ¹⁰ See

23 <https://www.facebook.com/business/help/2041148702652965?id=81885903231796>
 24 5 (last visited Nov. 8, 2023).

25 ¹¹ This Court will not have to look far to find evidence of Meta’s violations of
 26 privacy laws. Just in May of this year, the European Union fined Meta “a record-
 27 breaking” \$1.3 billion for violating EU privacy laws. See Hanna Ziady, *Meta*
slapped with record \$1.3 billion EU fine over data privacy,
<https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html> (last accessed Nov. 8, 2023).

1 Private Information had been impermissibly disclosed to an unauthorized third
2 party. In fact, Defendant **never** disclosed to Plaintiffs or Class Members that it
3 shared their sensitive and confidential communications, data and Private
4 Information with Facebook and other unauthorized third parties.¹²

5 30. Defendant's actions constitute an extreme invasion of Plaintiffs' and
6 Class Members' right to privacy and violate federal and state statutory and common
7 law as well as Defendant's statements Privacy Policy.¹³

8 31. As a result of Defendant's conduct, Plaintiffs and Class Members have
9 suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in
10 communicating with doctors online; (iii) emotional distress and heightened concerns
11 related to the release of Private Information to third parties; (iv) loss of the benefit
12 of the bargain; (v) diminution of value of the Private Information; (vi) statutory
13 damages and (vii) continued and ongoing risk to their Private Information. Plaintiffs
14 and Class Members have a substantial risk of future harm, and thus injury in fact,
15 due to the continued and ongoing risk of misuse of their Private Information that
16 Defendant shared with third parties.

17 32. Plaintiffs seek, on behalf of themselves and a class of similarly situated
18

19 ¹² In contrast to Defendant, in the last year, several medical providers that installed
20 the Meta Pixel on their Web Properties have provided their patients with notices of
21 data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g.,*
22 *Cerebral, Inc. Notice of HIPAA Privacy Breach*,
23 https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies*, FIERCE
24 HEALTHCARE (October 20, 2022), <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3>; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), <https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html>.

25
26
27
28 ¹³ AltaMed Privacy Policy, *supra* note 5.

1 persons, to remedy these harms and therefore assert the following statutory and
 2 common law claims against Defendant: (i) Violation of the California
 3 Confidentiality of Medical Information Act (“**CMIA**”), Cal. Civ. Code § 56, *et seq.*;
 4 (ii) Violation of the California Invasion of Privacy Act (“**CIPA**”), Cal. Penal Code
 5 § 630, *et seq.*; (iii) Violation of California’s Unfair Competition Law (“**UCL**”), Cal.
 6 Bus. & Prof. Code § 17200, *et seq.* – Unlawful and Unfair Business Practices;
 7 (iv) Common Law Invasion of Privacy; (v) Common Law Breach of Implied
 8 Contract; (vi) Violation of California Consumers Legal Remedies Act (“**CLRA**”),
 9 Cal. Civ. Code § 1750, *et seq.*; (vii) Negligence; (viii) Common Law Breach of
 10 Confidence, (ix) Common Law Breach of Fiduciary Duty; (x) Common Law Unjust
 11 Enrichment and (xi) violation of the Electronic Communications Privacy Act,
 12 18 U.S.C. §2511(3)(a), *et seq.*(“**ECPA**”).

PARTIES

14 33. Plaintiff L.V. is, and at all relevant times was, a California resident
 15 residing in Los Angeles County, California, where she intends to remain indefinitely.

16 34. Plaintiff S.T. is, and at all relevant times was, a California resident,
 17 residing in Orange County, California, where she intends to remain indefinitely.

18 35. Plaintiff C.R.T. is, and at all relevant times was, a California resident,
 19 residing in Los Angeles County, California, where she intends to remain indefinitely.

20 36. Defendant AltaMed is a not-for-profit organization providing healthcare
 21 services to patients in Los Angeles County, California. Defendant AltaMed was
 22 formed in California, with its principal place of business located at 1401 N
 23 Montebello Blvd., Montebello, CA 90640.

JURISDICTION & VENUE

24 37. This Court has jurisdiction over the subject matter of this action
 25 pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class
 26 exceeds \$5,000,000 exclusive of interest and costs, there are more than one hundred
 27 (100) putative class members defined below, and minimal diversity exists because a

1 significant portion of putative class members are citizens of a state different from
 2 the citizenship of at least one Defendant.

3 38. Pursuant to 28 U.S.C. Section 1331, this Court is the proper venue for
 4 this action because a substantial part of the events, omissions, and acts giving rise to
 5 the claims herein occurred in this District. Plaintiffs are citizens of California, reside
 6 in this District and used Defendant's Web Properties within this District. Moreover,
 7 Defendant received substantial compensation from offering healthcare services in
 8 this District, and Defendant made numerous misrepresentations which had a
 9 substantial effect in this District.

10 39. Defendant is subject to personal jurisdiction in California based upon
 11 sufficient minimum contacts that exist between Defendant and California.
 12 Defendant is incorporated in California, maintains its principal place of business in
 13 California, is authorized to conduct and is conducting business in California.

FACTUAL BACKGROUND

15 A. ***Defendant's Method of Transmitting Plaintiffs' & Class Members' Private***
 16 ***Information via the Meta Pixel.***

17 40. Defendant utilized Facebook advertisements and intentionally installed
 18 the Pixel and CAPI on its Web Properties.

19 41. As background, web communications consist of HTTP Requests and
 20 HTTP Responses, and any given browsing session may consist of thousands of
 21 individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- 22 a. **HTTP Request:** an electronic communication sent from the client
 23 device's browser to the website's server. GET Requests are one of
 24 the most common types of HTTP Requests. In addition to
 25 specifying a particular URL (i.e., web address), GET Requests can
 also send data to the host server embedded inside the URL, and can
 include cookies.¹⁴

27 ¹⁴ *An overview of HTTP*, MDN WEB DOCS, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview> (last visited Nov. 10, 2023).

- 1 b. **Cookies:** a small text file that can be used to store information on
 2 the client device which can later be communicated to a server or
 3 servers. Cookies are sent with HTTP Requests from client devices
 4 to the host server. Some cookies are “third-party cookies” which
 5 means they can store and communicate data when visiting one
 6 website to an entirely different website.¹⁵
- 1 c. **HTTP Response:** an electronic communication that is sent as a
 2 reply to the client device’s web browser from the host server in
 3 response to an HTTP Request. HTTP Responses may consist of a
 4 web page, another kind of file, text information, or error codes,
 5 among other data.¹⁶

7 42. A patient’s HTTP Request essentially asks Defendant’s Website to
 8 retrieve certain information, and the HTTP Response renders or loads the requested
 9 information in the form of “Markup” (the pages, images, words, buttons and other
 10 features that appear on the patient’s screen as they navigate Defendant’s Website).

11 43. Every website is comprised of Markup and “Source Code.” Source Code
 12 is a set of instructions that commands the website visitor’s browser to take certain
 13 actions when the web page first loads or when a specified event triggers the code.

14 44. Source Code may also command a web browser to send data
 15 transmissions to third parties in the form of HTTP Requests quietly executed in the
 16 background without notifying the web browser’s User. The Pixel incorporated by
 17 Defendant uses Source Code that does just that. The Pixel acts much like a traditional
 18 wiretap.

19 45. When patients visit Defendant’s Web Properties via an HTTP Request to
 20 Defendant’s server, that server sends an HTTP Response, including the Markup that
 21 displays the Webpage visible to the User and Source Code, including Defendant’s
 22 Pixel.

23 46. Thus, Defendant is, in essence, handing patients a tapped device and once

25 ¹⁵ *HTTP cookies*, MDN WEB DOCS, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies> (last visited Nov. 10, 2023).

27 ¹⁶ *An overview of HTTP*, *supra* note 13. One browsing session may consist of
 28 hundreds or thousands of individual HTTP Requests and HTTP Responses. *HTTP Messages*, MDN WEB DOCS, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages> (last visited Nov. 10, 2023).

the Webpage is loaded into the User’s browser, the software-based wiretap is invisibly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications—intended only for Defendant—and transmits those communications to third parties, including Facebook. Such conduct occurs on a continuous, and not sporadic, basis.

47. Defendant thus invites third parties, like Facebook, to place third-party cookies in the web browsers of Users logged into their services.

48. These cookies specifically identify the User and are sent with each intercepted communication to ensure the third party can uniquely identify the patient associated with the Private Information intercepted.

49. With substantial work and technical know-how, internet users can sometimes try to protect themselves from this browser-based wiretap technology and limit the data collected by tracking pixels. In response to this, Facebook created CAPI to make sure these attempts at protection are futile.

50. CAPI allows Facebook to continue to track user behavior even if users have turned off third-party cookies or limited data tracking on their devices.

51. Facebook’s CAPI is able to evade a Users’ attempts to protect their privacy because it does not intercept data communicated from the User’s browser. Instead, CAPI “is designed to create a direct connection between [Web hosts’] marketing data and [Facebook].”¹⁷

52. Thus, the communications between patients and Defendant, which are necessary to use Defendant's Web Properties, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

53. Client devices do not have access to Defendant's host servers and thus cannot prevent (or even detect) this transmission.

¹⁷ Michael Mata, *Stop Data Loss with Facebook Server-Side Tracking* (March 18, 2022), <https://madgicx.com/blog/facebook-server-side-tracking>.

1 54. While there is no way to confirm with certainty that a Web host like
 2 Defendant has implemented CAPI without access to the host server, companies like
 3 Facebook instruct Defendant to “[u]se the CAPI in addition to the [] Pixel, and share
 4 the same events using both tools,” because such a “redundant event setup” allows
 5 Defendant “to share website events [with Facebook] that the pixel may lose.”¹⁸

6 55. The third parties to whom a website transmits data through Pixels and
 7 associated workarounds like CAPI do not provide any substantive content relating to
 8 the User’s communications. Instead, these third parties are typically procured to track
 9 User data and communications for marketing purposes of the website owner (i.e., to
 10 bolster profits).

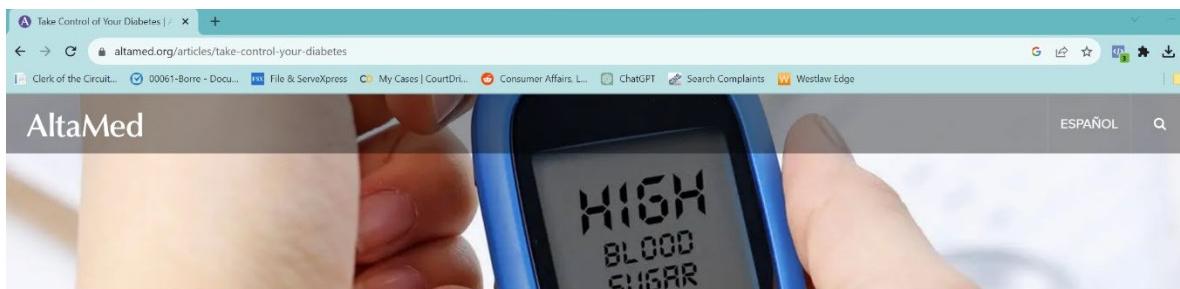
11 56. Thus, without any knowledge, authorization, or action by a User, a
 12 website owner like Defendant can use its source code to commandeer the User’s
 13 computing device, causing the device to contemporaneously and invisibly redirect the
 14 Users’ communications to third parties.

15 57. In this case, Defendant employed the Meta Pixel and CAPI to intercept,
 16 duplicate and redirect Plaintiffs’ and Class Members’ Private Information to
 17 Facebook.

18 58. For example, when a patient visits www.altamed.org and, after
 19 searching for information on diabetes, clicks on the page link for an article entitled
 20 “Take Control of Your Diabetes,” the patient’s browser automatically sends an
 21 HTTP request to AltaMed’s web server. AltaMed’s web server automatically
 22 returns an HTTP Response, which loads the markup for that particular webpage as
 23 depicted in ***Figure 1.***¹⁹

24
 25
 26 ¹⁸ See *Best Practices for Conversions API*, META,
 27 <https://www.facebook.com/business/help/308855623839366?id=818859032317965>
 (last visited Nov. 10, 2023).

28 ¹⁹ The image depicted in ***Figure 1*** was taken from
<https://www.altamed.org/articles/take-control-your-diabetes>



Take Control of Your Diabetes

April 30, 2018

Diabetes is one of the country's leading diseases, affecting one in 10 people in the U.S. However, by following a healthy diet and lifestyle, and receiving regular care, you can control diabetes before it affects your daily living.

What is diabetes

Diabetes affects your body's ability to use sugar to give you energy and keep you healthy. Insulin is a hormone produced in the pancreas that regulates the amount of sugar in your blood, and without the right level of insulin, your body cannot function properly. But medication and self-care can help you lead a long and healthy life.

Controlling diabetes risk

Diabetes is a serious health condition that puts you at higher risk for developing additional problems that can affect your vision, kidneys, blood vessels, and nervous system.

59. The patient visiting this particular web page only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

60. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that the patient is looking for treatment for his diabetes diagnosis — along with the patient's unique Facebook identifiers.

Figure 2: An HTTP single communication session sent from the device to Facebook that reveals the title of the article that the User clicked on ("take control

of your diabetes”), previous search terms (“diabetes management”) along with the User’s unique Facebook personal identifier (the c_user field).²⁰

²⁰ The images depicted in *Figures 2 and 3* were taken from <https://www.altamed.org/articles/take-control-your-diabetes>.

1 ***Figure 3. An easier-to-read representation of data sent to Facebook when a***
 2 ***User enters search terms into Defendant's search bar.***

```

 3           Query String Parameters view source view URL-encoded
 4           id: 1528202730787130
 5           ev: SubscribedButtonClick
 6           dl: https://www.altamed.org/articles/take-control-your-diabetes
 7           rl: https://www.altamed.org/search?keywords=diabetes+management
 8           if: false
 9           ts: 1699634276724
10          cd[buttonFeatures]: {"classList":"btn text-light dropdown-toggle show","destination":"","id":"dropdownSearchOpener","imageUrl":"","innerText":'\n      Open Search Form\n\n      \n      ','numChildButtons':0,"tag":"button","type":"button","name":"","value":""}
11          cd[buttonText]:
12           Open Search Form

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
  
```

cd[formFeatures]: []
 cd[pageFeatures]: {"title":"Take control of Your Diabetes | AltaMed"}
 cd[parameters]: []
 sw: 1664
 sh: 1110
 v: 2.9.138
 r: stable
 ec: 1
 o: 4126
 fbp: fb.1.1697199171995.1388383895
 ler: empty
 it: 1699634269343
 coo: false
 es: automatic
 tm: 3
 rqm: GET

16 61. Similarly, if a user navigates to the page displaying AltaMed's
 17 "Behavioral Health" services, including mental health services and suicide
 18 prevention, Defendant shares that information with Facebook, along with the User's
 19 personal identifiers – and along with the information that prior to this the patient
 20 was searching for a female doctor in Los Angeles specializing in addiction
 21 medicine.

1 ***Figure 4: An HTTP single communication session sent from the device to***
 2 ***Facebook that reveals the User's navigation to the Behavioral Health Services***
 3 ***page after searching for an Addiction Medicine specialist in LA, along with the***
 4 ***User's unique Facebook personal identifier (the c_user field).²¹***

5 ▼ Request Headers

:authority:	www.facebook.com
:method:	GET
:path:	/tr/?
	id=1528202730787130&ev=SubscribedButtonClick&dl=https%3A%
	2F%2Fwww.altamed.org%2Fbehavioral-health-
	services&xrl=https%3A%2F%2Fwww.altamed.org%2Ffind%2Fresults%6
	3Ftype%3Dspecialty%26specialty%63%0Addiction%2BMedicine%26ge
	nder%3DFemale%26language%3DEnglish%26keywords%3Dlos%2Fa
	ngeles%26affiliates%3Dyes&if=false&ts=1697564139758&cd[butto
	nFeatures]=%7B%22classList%22%3A%22%22%2C%22destination%
	22%3A%22tel%3A8002738255%22%2C%22id%22%3A%22%22%2C
	%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22(800)%
	20273-
	TALK%20(8255)%22%2C%22numChildButtons%22%3A0%2C%22tag
	%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A
	%22%22%7D&cd[buttonText]=(0)%200-
	TALK%20(0)&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%
	22title%22%3A%22Behavioral%20Health%20Services%22%7D&cd[pa
	rameters]=%5B%5D&sw=1664&sh=1110&v=2.9.134&r=stable&ec
	=1&o=30&fbp=fb.1.1697199171995.1388383895&ler=other&it=16
	97563962594&coo=false&es=automatic&tm=3&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0
	.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9,ru;q=0.8
Cookie:	datr=Qtl1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9IKWnpCg7UAhiJMv c_user=54 ; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A- 1%3A3037%3A%3AAcV1BceQuNe2NKPw6YQiRu6EdWJNipOXNWZs tb3j8Oo6; fr=0qDz5s2i5j2mlTx22.AWXOI_B7fc9zbcMpNXOBaw8cbdE.BIKEZm.- f.AAA.0.0.BIKEZm.AWVY2qk0kqo
Referer:	https://www.altamed.org/
Sec-Ch-Ua:	"Chromium";v="118", "Gooale Chrome";v="118", "Not=A?

21 The images depicted in **Figure 4** taken from <https://www.altamed.org/behavioral-health-services>.

1 62. Source Code can also execute command a website visitor's browser to
 2 send data transmissions to third parties via Pixels or web bugs,²² effectively open a
 3 spying window through which the webpage can funnel the visitor's data, actions and
 4 communications to third parties.

5 63. Looking at the previous example, Defendant's Source Code manipulates
 6 the patient's browser by secretly instructing it to report the patient's communications
 7 (HTTP Requests) to Facebook.

8 64. This occurs because the Pixel embedded in Defendant's Source Code is
 9 programmed to automatically track and transmit a patient's communications, and this
 10 occurs contemporaneously, invisibly and without the patient's knowledge.

11 65. Thus, without Users' consent, Defendant effectively uses this Source
 12 Code to commandeer patients' computing devices, thereby redirecting their Private
 13 Information to unauthorized third parties.

14 66. The information that Defendant's Pixel sends to Facebook includes,
 15 among other things, patients' PII, PHI and other confidential information.

16 67. Consequently, when Plaintiffs and Class Members visit Defendant's
 17 Website and communicate their Private Information, it is transmitted to Facebook,
 18 including, but not limited to, patient status, health conditions experienced and
 19 treatments sought, physician selected, appointments sought and specific button/menu
 20 selections. Each of these activities involves the transmission of sensitive information
 21 which is inevitably communicated to Facebook.

22 ***B. Defendant's Pixel Tracking Practices caused Plaintiffs' and Class Members'***
 23 ***Private Information to be sent to Facebook.***

24 68. Defendant utilizes Facebook's Business Tools and intentionally installed
 25 the Pixel and/or CAPI on its Web Properties to secretly track patients by recording
 26 their activity and experiences in violation of its common law, contractual, statutory

27 ²² These Pixels or web bugs are tiny image files that are invisible to website users.
 28 They are purposefully designed in this manner, or camouflaged, so that users remain
 unaware of them.

1 and regulatory duties and obligations.

2 69. Defendant's Web Properties contain a unique identifier which indicates
3 that a Meta Pixel is being used on a particular webpage.²³

4 70. The Pixels allow Defendant to optimize the delivery of advertisements,
5 measure cross-device conversions, create custom audiences and decrease advertising
6 and marketing costs.

7 71. However, Defendant's Web Properties do not need or rely on the Pixels
8 to function.

9 72. While seeking and using Defendant's services as a medical provider,
10 Plaintiffs and Class Members communicated their Private Information to Defendant
11 via its Web Properties.

12 73. Defendant did not disclose to Plaintiffs and Class Members that their
13 Private Information would be shared with Facebook as it was communicated to
14 Defendant. Rather, Defendant represented the opposite. This prevents the provision
15 of any informed consent by Plaintiffs or Class Members to Defendant for the
16 challenged conduct described herein.

17 74. Plaintiffs and Class Members never consented, agreed, authorized, or
18 otherwise permitted Defendant to disclose their Private Information to Facebook (or
19 any other third party), nor did they intend for Facebook to be a party to their
20 communications with Defendant. Defendant does not employ any form or click
21 system whereby Plaintiffs and Class Members provide their affirmative consent to
22 Defendant agreeing, authorizing, or otherwise permitting Defendant to disclose their
23 Private Information to Facebook (or any other third party).

24 75. Defendant's Pixels and CAPI sent sensitive Private Information to
25 Facebook, including but not limited to Plaintiffs' and Class Members': (i) status as
26

27 ²³ Inspection of Defendant's Source Code reveals that there are at least two Meta
28 Pixels embedded on its Web Properties, with ID numbers 1528202730787130 and
314921762413002.

1 medical patients; (ii) health conditions; (iii) sought treatment or therapies; (iv) sought
 2 providers and their specialties; (v) selected locations or facilities for treatment; and
 3 (vi) web pages viewed.

4 76. Importantly, the Private Information Defendant's Pixels sent to Facebook
 5 was sent alongside Plaintiffs' and Class Members' personal identifiers, including
 6 patients' IP address and cookie values such as the FID, thereby allowing individual
 7 patients' communications with Defendant, and the Private Information contained in
 8 those communications, to be linked to their unique Facebook accounts.

9 77. Through the Source Code deployed by Defendant, the cookies that they
 10 use to help Facebook identify patients include but are not necessarily limited to
 11 cookies named: "c_user," "datr," "fr," and "fbp."²⁴

12 78. The "c_user" cookie or FID is a type of third-party cookie assigned to
 13 each person who has a Facebook account, and it is composed of a unique and
 14 persistent set of numbers.

15 79. A User's FID is linked to their Facebook profile, which generally contains
 16 a wide range of demographics and other information about the User, including
 17 pictures, personal interests, work history, relationship status and other details.
 18 Because the User's Facebook Profile ID uniquely identifies an individual's Facebook
 19 account, Facebook—or any ordinary person—can easily use the Facebook Profile ID
 20 to quickly and easily locate, access and view the User's corresponding Facebook
 21 profile.

22 80. The "datr" cookie identifies the patient's specific web browser from
 23 which the patient is sending the communication. It is an identifier that is unique to the
 24 patient's specific web browser and is therefore a means of identification for Facebook

25 24 Defendant's Websites track and transmit data via first-party and third-party cookies.
 26 C_user, datr, and fr cookies are third-party cookies. The fbp cookie is a Facebook
 27 identifier that is set by Facebook source code and associated with Defendant's use of
 28 the Meta Pixel. The fbp cookie emanates from Defendant's Website as a putative first-
 party cookie, but is transmitted to Facebook through cookie syncing technology that
 hacks around the same-origin policy.

1 users. Facebook keeps a record of every datr cookie identifier associated with each of
 2 its users, and a Facebook user can obtain a redacted list of all datr cookies associated
 3 with his or her Facebook account from Facebook.

4 81. The “fr” cookie is a Facebook identifier that is an encrypted combination
 5 of the c_user and datr cookies.²⁵

6 ***C. Defendant’s Pixel Disseminates Patient Information Via Its Web Properties.***

7 82. By way of example, if a patient uses <https://www.altamed.org> to look
 8 for medical treatments, they may select “HIV Services” under the “Programs &
 9 Services” tab, which takes them to the list of services offered by Defendant to Users
 10 in need of HIV services. On those pages the User can further narrow their search
 11 results by the type of HIV services offered by Defendant.

12 83. The User’s selections and filters are transmitted to Facebook via the
 13 Meta Pixels, even if they contain the User’s treatment, procedures, medical
 14 conditions, or related queries, without alerting the User, and the images below
 15 confirm that the communications Defendant sends to Facebook contain the User’s
 16 Private Information and personal identifiers, including but not limited to their IP
 17 address, Facebook ID and datr and fr cookies, along with the search filters the User
 18 selected.

19 84. For example, a diabetes patient in search for HIV services can search for
 20 various HIV treatment options and information, from “HIV Prevention and Care”
 21 and “Testing” to “Sexual Health Campaigns.”²⁶

22
 23 ***Figure 5: Defendant’s transmission to Facebook of User’s navigating AltaMed’s***
 24 ***“HIV Services”***

25 See Gunes Acar et al., *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* 16 (March 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

26 See AltaMed HIV Services, <https://www.altamed.org/HIV>.

1	▼ Request Headers
2	:authority: www.facebook.com
3	:method: GET
4	:path: /tr/?
5	id=1528202730787130&ev=PageView&dl=https%3A%
6	2F%2Fwww.altamed.org%2FHIV&rl=https%3A%2F%2Fw
7	ww.altamed.org%2F&if=false&ts=1697563210903&sw=
8	1664&sh=1110&v=2.9.134&r=stable&ec=0&o=30&fbp
9	=fb.1.1697199171995.1388383895&ler=other&it=1697
10	563210803&coo=false&rqm=GET
11	:scheme: https
12	Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
13	Accept-Encoding: gzip, deflate, br
14	Accept-Language: en-US,en;q=0.9,ru;q=0.8
15	Cookie: datr=Qtl1Y1lVd2UWOuuBmn2Mb8vC;
16	sb=GrxtY1jj9IKWnpCg7UAhiJMv; c_user=540643061;
17	xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-

85. The first line of highlighted text, “id: 1528202730787130,” refers to Defendant’s Pixel ID for this particular Webpage and confirms that Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

86. In the second line of text, “ev:” is an abbreviation for event, and “PageView” is the type of event. Here, this event means that Defendant’s Pixel is sending information about the webpage being viewed, which can include information like page title, URL and page description.

87. The remaining lines of text identify the User as a patient: (i) seeking medical care from Defendant via www.AltaMed.org who is searching for HIV services.

88. Finally, the last line of highlighted text (“GET”), demonstrates that Defendant’s Pixel sent the User’s communications, and the Private Information

1 contained therein, alongside the User’s personal identifiers, including Facebook ID
2 and other cookies.

3 89. As mentioned above, if the patient selects other HIV services, that
4 selection is also automatically transmitted to Facebook by Defendant’s Pixels, along
5 with the patient’s personal identifiers. In addition to sharing patient’s conditions and
6 selected treatments via PageView and Microdata events, Defendant’s Pixels also
7 share the text of the buttons clicked by the patient via the “SubscribedButtonClick”
8 event.

9 90. For example, if a patient clicks on a button that contains a phone
10 number for a particular service, Defendant sends that information to Facebook via
11 the “SubscribedButtonClick” event, which shares the inner text of the button the
12 User clicked to schedule the procedure. In the figure below, AltaMed is disclosing
13 to Facebook that the user has clicked on the phone number for users to call if they
14 are “interested in starting or continuing HIV medical care.”

15
16
17
18
19
20
21
22
23
24
25
26
27
28

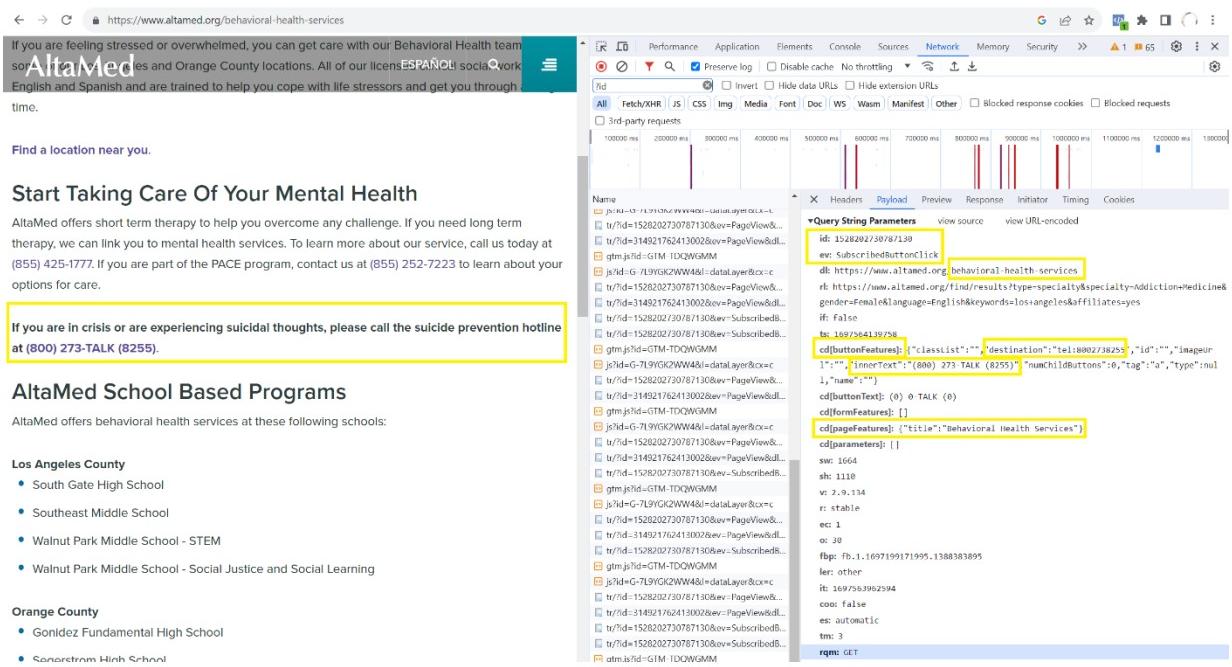
1
 2 ***Figures 6: HTTP communication sessions sent from the User's device to Facebook***
 3 ***revealing the inner text of the button clicked by the User, and their personal***
identifiers.

```
4   X Headers Payload Preview Response Initiator Timing Cookies
5
6   ▼Query String Parameters      view source      view URL-encoded
7
8     id: 1528202730787130
9     ev: SubscribedButtonClick
10    dl: https://www.altamed.org/HIV#slidein-content-modal-1660
11    rl: https://www.altamed.org/
12    if: false
13    ts: 1697563376787
14    cd[buttonFeatures]: {"classList": "", "destination": "tel:3238695448", "i
15      d": "", "imageUrl": "", "innerText": "(323) 869-5448", "numChildButtons": 0, "ta
16      g": "a", "type": null, "name": ""}
17    cd[buttonText]: (0) 0-0
18    cd[formFeatures]: []
19    cd[pageFeatures]: {"title": "HIV Prevention and Care Services"}
20    cd[parameters]: []
21    sw: 1664
22    sh: 1110
23    v: 2.9.134
24
25
26
27
28
```

18 91. As another example, if a User goes to AltaMed's website and searches
 19 for behavioral services, and then clicks on the link for a suicide prevention hotline,
 20 AltaMed shares all of that private information with Facebook.
 21
 22
 23
 24
 25
 26
 27
 28

1 ***Figures 7: HTTP communication sessions sent from the User's device to Facebook
revealing the service sought and the inner text of the button clicked by the User for
the suicide prevention hotline.***

2



14 ***Figures 8: An easier-to-read representation of HTTP communication sessions sent
from the User's device to Facebook revealing the inner text of the button clicked by
the User, and their personal identifiers.***

15

16

17

18

19

20

21

22

23

24

25

26

27

28

The figure shows a screenshot of a browser's developer tools Network tab, similar to Figure 7, but with the JSON payload displayed directly. The 'Payload' tab is active, showing the same JSON object as Figure 7, with the 'innerText' field of the 'buttonFeatures' object highlighted in yellow.

1 92. This information is automatically sent from the User's device to
 2 Facebook, and it reveals the User's FID (c_user field) along with each search filter
 3 the User selected.

4 93. A User who accesses Defendant's website while or having previously
 5 logged into Facebook will transmit the c_user cookie to Facebook, which contains
 6 that user's unencrypted Facebook ID, and other personal cookie values, including the
 7 datr and fr cookies.

8 94. When accessing www.AltaMed.org, for example, Facebook receives as
 9 many as nine (9) cookies, see **Figure 9** below:

Cookies	Name	Value	Domain	Expires / Max-Age
https://www.altamed.org	ar_debug	1	.doubleclick.net	/
https://td.doubleclick.net	sb	6Zc2ZdliKNMQ-s7vCP03lvO7	.facebook.com	/
https://pixel.sitescout.com	presence	C%7B%22t3%22%3A%5B%	.facebook.com	/
https://6514682.fl.doubleclick.net	fr	0WylTGvhNChW2084.AWV...	.facebook.com	/
Private state tokens	xs	37%3AWy_Pbx7xbS-E0g%3...	.facebook.com	/
Interest groups	c_user	61552747017033	.facebook.com	/
Shared storage	locale	en_US	.facebook.com	/
Cache storage	wd	1600x910	.facebook.com	/
Background services	dpr	1.5	.facebook.com	/
	datr	65c2ZU8pUo0fktnKWDa8a...	.facebook.com	/

15 95. The fr cookie contains, at least, an encrypted Facebook ID and browser
 16 identifier.²⁷ Facebook, at a minimum, uses the fr cookie to identify Users.²⁸

17 96. At each stage, Defendant AltaMed also utilized the _fbp cookie, which
 18 attaches to a browser as a first-party cookie, and which Facebook uses to identify a
 19 browser and a User, see **Figure 10** below:²⁹

Name	Value	Domain	Expires / Max-Age
_fbp	fb.1.1697572660446.16521...	.altamed.org	/ 2024-01-23T17:17:04.000Z

24 27 Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit 33*
 25 (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

26 28 *Cookies Policy*, META, <https://www.facebook.com/policy/cookies/> (last visited
 27 Nov. 10, 2023).

28 29 *Id.*

1
2 97. The fr cookie expires after ninety (90) days unless the User's browser
3 logs back into Facebook.³⁰ If that happens, the time resets, and another ninety (90)
4 days begins to accrue.

5 98. The _fbp cookie expires after ninety (90) days unless the User's browser
6 accesses the same website.³¹ If that happens, the time resets, and another ninety (90)
7 days begins to accrue.

8 99. The Facebook Meta Pixel uses both first- and third-party cookies. A first-
9 party cookie is "created by the website the user is visiting"—i.e., Defendant.³²

10 100. A third-party cookie is "created by a website with a domain name other
11 than the one the user is currently visiting"—i.e., Facebook.³³

12 101. The _fbp cookie is always transmitted as a first-party cookie.

13 102. Facebook, at a minimum, uses the fr, _fbp and c_user cookies to link to
14 FIDs and corresponding Facebook profiles.

15 103. As shown in the figures above, Defendant sent these identifiers with the
16 event data.

17 104. Plaintiffs never consented, agreed, authorized, or otherwise permitted
18 Defendant to disclose their Private Information, nor did they authorize any assistance
19 with intercepting their communications.

20 105. Plaintiffs were never provided with any written notice that Defendant
21 disclosed their Private Information, nor were they provided with any means of opting
22 out of such disclosures.

23 106. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs'

24 ³⁰ *Id.*

25 ³¹ *Id.*

26 ³² This is confirmable by using developer tools to inspect a website's cookies and
27 track network activity.

28 ³³ This is confirmable by tracking network activity.

1 Private Information to Facebook.

2 **D. Defendant Violates Its Promises to Users and Patients to Protect Their
3 Confidentiality.**

4 107. Defendant does not have the legal right to use or share Plaintiffs' and
5 Class Members' data, because this information is protected by the Health Insurance
6 Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule. The Privacy
7 Rule does not permit the use and disclosure of Private Information to Facebook for
8 use in targeted advertising.³⁴

9 108. Beyond Defendant's legal obligations to protect the confidentiality of
10 individuals' Private Information, Defendant's privacy policies and online
11 representations affirmatively and unequivocally state that any personal information
12 provided to Defendant will remain secure and protected.

13 109. AltaMed's "Notice of Privacy Practices" informs Users that AltaMed "is
14 committed to safeguarding your protected health information," that "AltaMed will
15 only use or share your health information if it is needed to provide you with health
16 services," and that "uses and sharing of your PHI for marketing purposes would
17 require your prior written authorization."³⁵ No mention of Facebook or its Pixel is
18 made in AltaMed's Privacy Policy or website, and there is no indication that AltaMed
19 will be in the business of transmitting its Users PHI to third parties via its website.³⁶

20 110. Defendant has unequivocally failed to adhere to its promises vis-à-vis its
21 duty to safeguard Private Information of its Users. Defendant has made its Privacy
22 Policy available on its websites. Defendant includes these privacy policies and
23 commitments to maintain the confidentiality of its Users' sensitive information as
24 terms of its contracts with those Users, including contracts entered with Plaintiffs and

25
26³⁴ See 45 C.F.R. § 164.502.
27³⁵ AltaMed Privacy Policy, *supra* note 5.
28³⁶ *Id.*

1 the Class Members. In these contract terms and other representations to Plaintiffs and
 2 Class Members and the public, Defendant promised to take specific measures to
 3 protect Plaintiffs' and Class Members' Private Information, consistent with industry
 4 standards and federal and state law. However, it failed to do so.

5 111. Even non-Facebook users can be individually identified via the
 6 information gathered on the Digital Platforms, like an IP address or personal device
 7 identifying information. This is precisely the type of information for which HIPAA
 8 requires the use of de-identification techniques to protect patient privacy.³⁷

9 112. In fact, in an action currently pending against Facebook related to use of
 10 their Pixel on healthcare provider web properties, Facebook explicitly stated it
 11 requires Pixel users to "post a prominent notice on every page where the Pixel is
 12 embedded and to link from that notice to information about exactly how the Pixel
 13 works and what is being collected through it, so it is not invisible."³⁸ Defendant did
 14 not post such a notice.

15 113. Facebook further stated that "most providers [...] will not be sending
 16 [patient information] to Meta because it violates Meta's contracts for them to be doing
 17 that."³⁹

18 114. Despite a lack of disclosure, Defendant allowed third parties to "listen in"
 19 on patients' confidential communications and to intercept and use for advertising
 20

21
 22 ³⁷ *Guidance Regarding Methods for De-identification of Protected Health*
Information in Accordance with the Health Insurance Portability and Accountability
Act (HIPAA) Privacy Rule, U.S. DEP'T OF HEALTH AND HUM. SERVICES,
<https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Nov. 10, 2023).

23
 24
 25 ³⁸ See Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in
In re Meta Pixel Healthcare Litig., Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9,
 26 2022) (Hon. J. Orrick), at 19:12-18; see also *In re Meta Pixel Healthcare Litig.*, 2022
 27 WL 17869218 (N.D. Cal. Dec 22, 2022).

28 ³⁹ *Id.* at 7:20-8:11.

1 purposes the very information they promised to keep private, in order to bolster their
2 profits.

3 ***E. Plaintiffs' and Class Members Reasonably Believed That Their Confidential***
4 ***Medical Information Would Not Be Shared with Third Parties.***

5 115. Plaintiffs and Class Members were aware of Defendant's duty of
6 confidentiality when they sought medical services from Defendant.

7 116. Indeed, at all times when Plaintiffs and Class Members provided their
8 Private Information to Defendant, they each had a reasonable expectation that the
9 information would remain confidential and that Defendant would not share the Private
10 Information with third parties for a commercial purpose, unrelated to patient care.

11 117. Personal data privacy and obtaining consent to share Private Information
12 are material to Plaintiffs and Class Members.

13 118. Plaintiffs and Class Members relied to their detriment on Defendant's
14 uniform representations and omissions regarding protection privacy, limited uses and
15 lack of sharing of their Private Information.

16 119. Now that their sensitive personal and medical information is in possession
17 of third parties, Plaintiffs and Class Members face a constant threat of continued
18 harm—including bombardment of targeted advertisements based on the unauthorized
19 disclosure of their personal data. Collection and sharing of such sensitive information
20 without consent or notice poses a great threat to individuals by subjecting them to the
21 never-ending threat of identity theft, fraud, phishing scams and harassment.

22 ***F. Defendant Violated HIPAA.***

23 120. Defendant's disclosure of Plaintiffs' and Class Members' Private
24 Information to entities like Facebook also violated HIPAA.

25 121. Under federal law, a healthcare provider may not disclose PII, non-
26 public medical information about a patient, potential patient, or household member

1 of a patient for marketing purposes without the patient's express written
 2 authorization.⁴⁰

3 122. Guidance from the United States Department of Health and Human
 4 Services instructs healthcare providers that patient status alone is protected by
 5 HIPAA.

6 123. In Guidance regarding Methods for De-identification of Protected
 7 Health Information in Accordance with the HIPAA Privacy Rule, the Department
 8 instructs:

9 Identifying information alone, such as personal names,
 10 residential addresses, or phone numbers, would not
 11 necessarily be designated as PHI. For instance, if such
 12 information was reported as part of a publicly accessible data
 13 source, such as a phone book, then this information would not
 14 be PHI because it is not related to health data... If such
 15 information was listed with health condition, health care
 16 provision, or payment data, such as an indication that the
 17 individual was treated at a certain clinic, then this information
 18 would be PHI.⁴¹

19 124. In its guidance for Marketing, the Department further instructs:

20 The HIPAA Privacy Rule gives individuals important
 21 controls over whether and how their protected health
 22 information is used and disclosed for marketing purposes.
 23 With limited exceptions, the Rule requires an individual's
 24 written authorization before a use or disclosure of his or her
 25 protected health information can be made for marketing. ...
 26 Simply put, a covered entity may not sell protected health
 27 information to a business associate or any other third party for
 28 that party's own purposes. Moreover, *covered entities may
 not sell lists of patients to third parties without obtaining*

⁴⁰ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

⁴¹https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 7, 2023).

1 authorization from each person on the list. (Emphasis
 2 added).⁴²

3 125. Under HIPAA, an IP address is considered PII: HIPAA defines PII to
 4 include “any unique identifying number, characteristic or code” and specifically
 lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

5 126. HIPAA further declares information as personally identifiable where the
 6 covered entity has “actual knowledge that the information could be used alone or in
 7 combination with other information to identify an individual who is a subject of the
 8 information.” 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

9 127. Facebook, Google and other third-party marketing companies track IP
 10 addresses to track and target individual homes and their occupants with advertising.

11 128. Consequently, Defendant’s disclosure of patients’ IP addresses violated
 12 HIPAA and industry privacy standards.

13 129. Defendant’s placing of third-party tracking code on its Web Properties
 14 is a violation of Plaintiffs’ Class Members’ privacy rights under federal law.⁴³

15 ***G. Defendant Violated Industry Standards.***

16 130. A medical provider’s duty of confidentiality is embedded in the
 17 physician-patient and hospital-patient relationship—it is a cardinal rule.

18 131. The American Medical Association’s (“AMA”) Code of Medical Ethics
 19 contains numerous rules protecting the privacy of patient data and communications.

20 132. AMA Code of Ethics Opinion 3.1.1 provides:

21 Protecting information gathered in association with the care
 22 of the patient is a core value in health care... Patient privacy

23
 24
 25
 26 ⁴²<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (last visited Nov. 7, 2023).

27 ⁴³ While Plaintiffs do not bring a claim under HIPAA itself, this violation evidences
 28 Defendant’s wrongdoing as relevant to other claims.

1 encompasses a number of aspects, including, ... personal data
2 (informational privacy)[.]⁴⁴

3 133. AMA Code of Medical Ethics Opinion 3.2.4 provides:

4 Information gathered and recorded in association with the
5 care of the patient is confidential. Patients are entitled to
6 expect that the sensitive personal information they divulge
7 will be used solely to enable their physician to most
8 effectively provide needed services. Disclosing information
9 for commercial purposes without consent undermines trust,
10 violates principles of informed consent and confidentiality,
11 and may harm the integrity of the patient-physician
12 relationship. Physicians who propose to permit third-party
13 access to specific patient information for commercial
14 purposes should: (a) Only provide data that has been de-
15 identified. [and] (b) Fully inform each patient whose record
16 would be involved (or the patient's authorized surrogate when
17 the individual lacks decision-making capacity about the
18 purposes for which access would be granted.⁴⁵

19 134. AMA Code of Medical Ethics Opinion 3.3.2 provides:

20 Information gathered and recorded in association with the
21 care of a patient is confidential, regardless of the form in
22 which it is collected or stored. Physicians who collect or store
23 patient information electronically...must: (c) Release patient
24 information only in keeping with ethics guidelines for
25 confidentiality.⁴⁶

26 ***H. Defendant was Unjustly Enriched from the Use of The Pixel.***

27 135. The primary motivation and a determining factor in Defendant's
28 interception and disclosure of Plaintiffs' and Class Members' Private Information
was to commit criminal and tortious acts in violation of federal and state laws as

26 ⁴⁴<https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf> (last visited Nov. 8, 2023).

27 ⁴⁵ *Id.*

28 ⁴⁶ *Id.*

1 alleged herein, namely, the use of patient data for advertising in the absence of
2 express written consent.

3 136. Defendant's further use of the Private Information after the initial
4 interception and disclosure for marketing and revenue generation was in violation of
5 HIPAA and an invasion of privacy. In exchange for disclosing its patients' PII,
6 Defendant is compensated by Facebook in the form of enhanced advertising
7 services and more cost-efficient marketing on Facebook.

8 137. Upon information and belief, Defendant was advertising its services on
9 Facebook, and the Pixel was used to "help [Defendant] understand the success of
10 [its] advertisement efforts on Facebook."

11 138. Retargeting is a form of online marketing that targets users with ads
12 based on their previous Internet communications and interactions.

13 139. Upon information and belief, Defendant re-targeted patients and
14 potential patients to get more patients to use its services.

15 140. By utilizing the Pixel, the cost of advertising and retargeting was
16 reduced, thereby benefitting Defendant.

17 **I. Plaintiffs' Private Information Has Value**

18 141. Facebook is one of the largest advertising companies in the country,
19 with over 2.9 billion active users.⁴⁷

20 142. Realizing the value of having direct access to millions of consumers, in
21 2007, Facebook began monetizing its platform by launching "Facebook Ads,"
22 proclaiming it to be a "completely new way of advertising online" that would allow
23 "advertisers to deliver more tailored and relevant ads."⁴⁸

24
25

⁴⁷ S. Dixon, *Facebook Users by Country 2023*, STATISTA (February 24, 2023),
26 www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.

27
28

⁴⁸ *Facebook Unveils Facebook Ads*, META (November 6, 2007),
<https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>.

1 143. Given the highly specific data used to target specific users, it is no
 2 surprise that millions of companies and individuals utilize Facebook's advertising
 3 services. Meta generates almost all of its revenue from selling advertisement
 4 placements, as depicted in ***Figure 7***:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2023 Q1	\$28.65 billion	\$28.101 billion	98.1%
2022	\$116.61 billion	\$113.64 billion	97.5%
2021	\$117.93 billion	\$114.93 billion	97.46%
2020	\$85.97 billion	\$84.17 billion	97.90%
2019	\$70.70 billion	\$69.66 billion	98.52%
2018	\$55.84 billion	\$55.01 billion	98.51%

11 144. One of its most powerful advertising tools is Meta Pixel, formerly
 12 known as Meta Pixel, which launched in 2015.

13 145. Ad Targeting has been extremely successful due, in large part, to
 14 Facebook's ability to target people at a granular level. "Among many possible target
 15 audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose
 16 activity on Facebook suggests that they're more likely to engage with/distribute
 17 liberal political content' and nearly seven million Facebook users who 'prefer high-
 18 value goods in Mexico.'"⁴⁹

19 146. Acknowledging that micro-level targeting is highly problematic, in
 20 November of 2021, Facebook announced that it was removing options that "relate to
 21 topics people may perceive as sensitive," such as "Health causes (e.g., 'Lung cancer
 22 awareness', 'World Diabetes Day', 'Chemotherapy'), Sexual orientation (e.g.,
 23 'same-sex marriage' and 'LGBT culture'), "Religious practices and groups" (e.g.,
 24 'Catholic Church' and 'Jewish holidays') as well as "Political beliefs, social issues,
 25 causes, organizations, and figures."

26 49 Natasha Singer, *What You Don't Know about How Facebook Uses Your Data*,
 27 N.Y. TIMES (April 11, 2018),
 28 <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>.

1 147. For Facebook, the Pixel acts as a conduit of information. If the User has
 2 a Facebook account, the Private Information collected is linked to the individual
 3 Users' Facebook account.

4 148. Facebook can also link the data to a users' Facebook account through
 5 the "Facebook Cookie," which is a workaround to recent cookie-blocking
 6 techniques, including one developed by Apple, Inc., to track users.⁵⁰

7 149. The collection and use of this data raises concerns about user privacy
 8 and the potential misuse of personal information. For example, when Users browse
 9 Defendant's Web Properties, every bit of their activity is tracked and monitored. By
 10 analyzing this data using algorithms and machine learning techniques, these entities
 11 tracking this information can learn a chilling level of detail about Users' behavioral
 12 patterns, preferences and interests.

13 150. While this data can be used to provide personalized and targeted content
 14 and advertising, it can also be used for more nefarious purposes, such as tracking
 15 and surveillance. For example, if an advertiser or social media platform has access
 16 to a User's browsing history, search queries and social media activity, they could
 17 potentially build a detailed profile of that User's behavior patterns, including where
 18 they go, what they do and who they interact with.

19 151. This level of surveillance and monitoring raises important ethical and
 20 legal questions about privacy, consent and the use of personal data. It is important
 21 for Users to be aware of how their data is being collected and used and to have
 22 control over how their information is shared and used by advertisers and other
 23 entities.

24 152. Investigative journalists have published several reports detailing the
 25 seemingly ubiquitous use of tracking technologies on hospitals', health care
 26

27 ⁵⁰ Maciej Zawadziński & Michal Włosik, *What Facebook's First-Party Cookie*
 28 *Means for AdTech*, CLEAR CODE (June 8, 2022), <https://clearcode.cc/blog/facebook-first-party-cookie-adtech/>.

1 providers' and telehealth companies' digital properties to surreptitiously capture and
 2 to disclose their users' Private Information.

3 153. Specifically, and for example, The Markup reported that 33 of the largest
 4 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet
 5 of data whenever a person clicked a button to schedule a doctor's appointment.⁵¹
 6 Estimates are that over 664 hospital systems and providers utilize some form of
 7 tracking technology on their digital properties.⁵²

8 154. David Holtzman, a health privacy consultant, was "deeply troubled" by
 9 the results of The Markup's investigation and indicated "it is quite likely a HIPAA
 10 violation" by the hospitals, such as Defendant.⁵³

11 155. Laura Lazaro Cabrera, a legal officer at Privacy International, indicated
 12 that Facebook's access to use even only some of these data points—such as just the
 13 URL—is problematic. She explained, "Think about what you can learn from a URL
 14 that says something about scheduling an abortion' . . . 'Facebook is in the business
 15 of developing algorithms. They know what sorts of information can act as a proxy
 16 for personal data."⁵⁴

17
 18 ⁵¹ Todd Feathers, *et al.*, *Facebook Is Receiving Sensitive Medical Information from*
 19 *Hospital Websites*, THE MARKUP (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

20
 21 ⁵² Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action*
 22 *over Meta's alleged patient data mining*, FIERCE HEALTHCARE (November 4, 2022),
<https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook>.

23
 24 ⁵³ *Id.*

25
 26 ⁵⁴ Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are*
 27 *Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (Sept. 25,
 28 2022), <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>.

1 156. Moreover, the misuse of this data could lead to the spread of false or
 2 misleading information, which could have serious consequences, particularly in the
 3 case of health-related information. As an example, the Cambridge Analytica scandal
 4 revealed that personal data was misused to target individuals with political
 5 propaganda and misinformation.⁵⁵

6 157. The Cambridge Analytica scandal involved the misuse of personal data
 7 collected from Facebook users, which was then used to target individuals with
 8 political advertising and propaganda. The scandal highlighted the potential dangers
 9 of using personal data for targeted advertising and the need for greater transparency
 10 and accountability in the collection and use of personal information.⁵⁶ One of the
 11 ways that Cambridge Analytica was able to collect personal data was third-party
 12 apps that collected data from users and their friends. This data was then used to
 13 build detailed profiles of individuals, which were used to target them with
 14 personalized political ads and propaganda.

15 158. The use of algorithms and machine learning techniques to analyze this
 16 data allowed Cambridge Analytica to identify patterns in users' behavior and
 17 preferences, which were then used to target them with specific messages and ads.

18 159. This highlights the potential dangers of using personal data to build
 19 detailed profiles of individuals, particularly when that data is collected without their
 20 knowledge or consent. It also raises important questions about the ethics of using
 21 personal data for political purposes and the need for greater regulation and oversight
 22 of data collection and use.

23
 24
 25 ⁵⁵ Sam Meredith, *Here's Everything You Need to Know about the Cambridge*
 26 *Analytica Scandal*, CNBC (March 23, 2018),
<https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html>.

27
 28 ⁵⁶ *Id.*

1 160. As pointed out by the OCR, impermissible disclosures of data in the
 2 healthcare context “may result in identity theft, financial loss, discrimination,
 3 stigma, mental anguish, or other serious negative consequences to the reputation,
 4 health, or physical safety of the individual or to others identified in the individual’s
 5 PHI.... This tracking information could also be misused to promote misinformation,
 6 identity theft, stalking, and harassment.”⁵⁷

7 161. Finally, as Judge Orrick pointed out in a recent decision allowing claims
 8 under California and common law against Regents of the University of California
 9 for collecting personal medical data via the Meta Pixel to go forward, “[p]ersonal
 10 medical information is understood to be among the most sensitive information that
 11 could be collected about a person” and unauthorized transmission or interception of
 12 such data by third parties may constitute a “highly offensive” intrusion of privacy.

13 *Doe v. Regents of Univ. of Cal.*, 23-cv-00598-WHO (N.D. Cal. May 6, 2023).

14 ***J. Plaintiffs and Class Members Have a Reasonable Expectation of Privacy in
 15 Their Private Information, Especially with Respect to Sensitive Medical
 16 Information.***

17 162. Plaintiffs and Class Members have a reasonable expectation of privacy
 18 in their Private Information, including personal information and sensitive medical
 19 information.

20 163. Patient PHI specifically is protected by federal law under HIPAA.

21 164. HIPAA sets national standards for safeguarding protected health
 22 information. For example, HIPAA limits the permissible use of health information
 23 and prohibits the disclosure of this information without explicit authorization. See
 24 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement
 25 appropriate safeguards to protect this information. See 45 C.F.R. § 164.530(c)(1).

26 ⁵⁷ See *Use of Online Tracking Technologies by HIPAA Covered Entities and*
 27 *Business Associates*, available at [https://www.hhs.gov/hipaa/for-](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html)
 28 *professionals/privacy/guidance/hipaa-online-tracking/index.html* (last visited Nov.
 7, 2023) (emphasis added).

1 165. Because federal legal framework applies to health care providers,
 2 including Defendant, Plaintiffs and the members of the Class had a reasonable
 3 expectation of privacy over their PHI.

4 166. Privacy polls and studies uniformly show that the overwhelming
 5 majority of Americans consider one of the most important privacy rights to be the
 6 need for an individual's affirmative consent before a company collects and shares its
 7 customers' data.

8 167. For example, a recent study by Consumer Reports shows that 92% of
 9 Americans believe that internet companies and websites should be required to
 10 obtain consent before selling or sharing consumers' data, and the same percentage
 11 believe internet companies and websites should be required to provide consumers
 12 with a complete list of the data that has been collected about them.⁵⁸ Moreover,
 13 according to a study by Pew Research Center, a majority of Americans,
 14 approximately 79%, are concerned about how data is collected about them by
 15 companies.⁵⁹

16 168. Medical data is even more valuable because unlike other personal
 17 information, such as credit card numbers that can be quickly changed, medical data
 18 is static. This is why companies possessing medical information, like Defendant, are
 19 intended targets of cyber-criminals.⁶⁰

20 ⁵⁸ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New*
 21 *Survey Finds*, CONSUMER REPORTS (May 11, 2017),
<https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

23 ⁵⁹ *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over*
 24 *Their Personal Information*, PEW RESEARCH CENTER (November 15, 2019),
<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

26 ⁶⁰ Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than*
 27 *your credit card*, REUTERS (September 24, 2014),
<https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924>.

1 169. Patients using Defendant's Web Properties must be able to trust that the
 2 information they input, including their physicians, their health conditions and
 3 courses of treatment will be protected. Indeed, numerous state and federal laws
 4 require this. And these laws are especially important when protecting individuals
 5 with particular medical conditions, such as HIV or AIDS that can and do subject
 6 them to regular discrimination. Furthermore, millions of Americans keep their
 7 health information private because it can become the cause of ridicule and
 8 discrimination.

9 170. Other privacy law experts have expressed concerns about the disclosure
 10 to third parties of a users' sensitive medical information. For example, Dena
 11 Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current
 12 Director of Health Policy and Data Governance at Elektra Labs—explained that
 13 having your personal health information disseminated in ways you are unaware of,
 14 could have serious repercussions, including affecting your ability to obtain life
 15 insurance and how much you pay for that coverage, increase the rate you are
 16 charged on loans, and leave you vulnerable to workplace discrimination.⁶¹

17 171. A 2021 report by Invisibly found that personal medical information is
 18 one of the most valuable pieces of information within the market for data. The
 19 report noted that “[i]t’s worth acknowledging that because health care records often
 20 feature a more complete collection of the PII User’s identity, background, and
 21 personal identifying information (PII), health care records have proven to be of
 22 particular value for data thieves. While a single social security number might go for
 23 \$0.53, a complete health care record sells for \$250 on average.⁶²

24 ⁶¹ See Class Action Complaint, *Jane Doe v. Regents of the Univ. of Cal. d/b/a UCSF*

25 *Medical Center*, CLASS ACTION (Feb. 9, 2023),
 26 <https://www.classaction.org/media/doe-v-regents-of-the-university-of-california.pdf>.

27 ⁶² *Exploring the Economics of Personal Data: A Survey of Methodologies for*
 28 *Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, NO. 220

1 172. Defendant surreptitiously collected and used Plaintiffs' and Class
2 Members' Private Information, including highly sensitive medical information,
3 through Meta Pixel in violation of Plaintiffs' and Class Members' privacy interests.

4 **REPRESENTATIVE PLAINTIFFS' EXPERIENCES**

5 **Plaintiff L.V.**

6 173. Plaintiff L.V. has been a patient at AltaMed since at least 2018. Plaintiff
7 L.V. started using the AltaMed website in 2020, utilizing the Web Properties many
8 times in recent years. Plaintiff L.V. has had a Facebook account for about ten years
9 and started to receive unsolicited advertisements relating to her medical conditions
10 shortly after visiting AltaMed's Web Properties.

11 174. Defendant encouraged Plaintiff L.V. to utilize AltaMed's Website and
12 online portal in order to search for doctors, make appointments, review medical
13 treatments, her medications, and to review test results from previous exams.

14 175. While using Defendant's Web Properties, Plaintiff L.V. communicated
15 sensitive—and what she expected to be confidential—personal and medical
16 information to Defendant.

17 176. Plaintiff L.V. used AltaMed's Web Properties to research healthcare
18 providers and communicate with them, research particular medical concerns and
19 treatments, fill out forms and questionnaires, schedule and attend appointments
20 including for thyroid treatment, hair loss, bariatric surgery, a yeast infection and to
21 test for breast cancer and perform other tasks related to her specific medical inquiries
22 and treatment.

23 177. Plaintiff L.V. also utilized AltaMed's Patient Portal to see test results,
24 obtain medical history, message doctors and order medications related to the above
25 listed health conditions.

26
27
28

(Apr. 2, 2013) https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Nov. 8, 2023).

1 178. While using AltaMed's digital services, Plaintiff L.V. communicated and
2 received information regarding her appointments, treatments, medications and
3 clinical information. As a result of Defendant choosing to install the Pixel and other
4 tracking technologies on its Web Properties, this information was intercepted, viewed,
5 analyzed and used by unauthorized third parties.

6 179. Plaintiff L.V. accessed AltaMed's Web Properties in connection with
7 receiving healthcare services from AltaMed or AltaMed's affiliates at AltaMed's
8 direction and with AltaMed's encouragement.

9 180. Plaintiff L.V. has used and continues to use the same devices to maintain
10 and to access an active Facebook account throughout the relevant period.

11 181. Plaintiff L.V. noticed that she began receiving targeted advertising on
12 Facebook directed to her medical conditions and treatments shortly after disclosing
13 information regarding those same medical conditions on AltaMed's website.

14 182. For example, in 2022 and around September 2023, after looking for
15 information about her thyroid condition on AltaMed's website and getting a
16 prescription medication from Defendant, she began receiving advertisements on
17 Facebook for the same thyroid medication she was prescribed at AltaMed. In 2020
18 Plaintiff L.V. also began getting advertisements on Facebook regarding breast cancer
19 after she went to Defendant for a biopsy of her breast lump.

20 183. As a medical patient using AltaMed's health services, Plaintiff L.V.
21 reasonably expected that her online communications with AltaMed were solely
22 between herself and AltaMed, and that such communications would not be
23 transmitted or intercepted by a third party. Plaintiff L.V. also relied on AltaMed's
24 Privacy Policies in reasonably expecting AltaMed would safeguard her Private
25 Information. But for her status as AltaMed's patient and its representations via its
26 Privacy Policies, Plaintiff L.V. would not have disclosed her Private Information to
27 AltaMed.

28

1 **Plaintiff S.T.**

2 184. Plaintiff S.T. has been a patient at AltaMed in Southern California since
3 at least 2013. Plaintiff S.T. started using the AltaMed website around the same time
4 she became a patient, utilizing the Web Properties many times in recent years.
5 Plaintiff S.T. has had a Facebook account for approximately 15 years and started to
6 receive unsolicited advertisements relating to her medical condition, including but not
7 limited to, shortly after visiting AltaMed's Web Properties.

8 185. Defendant encouraged Plaintiff S.T. to utilize AltaMed's Web Properties
9 in order to search for doctors, make appointments, review medical treatments and to
10 review charts from previous exams.

11 186. While using Defendant's Web Properties, Plaintiff S.T. communicated
12 sensitive—and what she expected to be confidential—personal and medical
13 information to Defendant.

14 187. Plaintiff S.T. used AltaMed's Web Properties to research healthcare
15 providers, research particular medical concerns and treatments, fill out forms and
16 questionnaires, schedule and attend appointments and perform other tasks related to
17 her specific medical inquiries and treatment.

18 188. Plaintiff S.T. visited Defendant's facilities many times for medical
19 treatments related to her endometrial cancer and had a hysterectomy in October 2022
20 at Defendant's facilities.

21 189. While using AltaMed's Web Properties, Plaintiff S.T. communicated and
22 received information regarding her appointments, treatments, medications and
23 clinical information, including her surgeries, lab work and scans. As a result of
24 Defendant choosing to install the Pixel and other tracking technologies on its Web
25 Properties, this information was intercepted, viewed, analyzed and used by
26 unauthorized third parties.

1 190. Plaintiff S.T. accessed AltaMed's Web Properties in connection with
2 receiving healthcare services from AltaMed or AltaMed's affiliates at AltaMed's
3 direction and with AltaMed's encouragement.

4 191. Plaintiff S.T. has used and continues to use the same devices to maintain
5 and to access an active Facebook account throughout the relevant period.

6 192. Plaintiff S.T. noticed that she began receiving targeted advertising on
7 Facebook directed to her medical condition after researching information regarding
8 those same medicals condition on AltaMed's website.

9 193. For example, after looking for information about endometrial fibroids on
10 AltaMed's website, she began receiving advertisements on Facebook related to
11 endometrial fibroids.

12 194. As a medical patient using AltaMed's health services, Plaintiff S.T.
13 reasonably expected that her online communications with AltaMed were solely
14 between herself and AltaMed, and that such communications would not be
15 transmitted or intercepted by a third party. Plaintiff S.T. also relied on AltaMed's
16 Privacy Policies in reasonably expecting AltaMed would safeguard her Private
17 Information. But for her status as AltaMed's patient and its representations via its
18 Privacy Policies, Plaintiff S.T. would not have disclosed her Private Information to
19 AltaMed.

20 **Plaintiff C.R.T**

21 195. Plaintiff C.R.T. has been a patient at AltaMed in Southern California for
22 almost two years. Plaintiff C.R.T. started using the AltaMed website in March of
23 2022, utilizing the Web Properties many times in the last year. Plaintiff C.R.T. has
24 had a Facebook account since 2009 and started to receive unsolicited advertisements
25 relating to her medical condition shortly after visiting AltaMed's Web Properties.

26 196. Defendant encouraged Plaintiff C.R.T. to utilize AltaMed's Web
27 Properties in order to search for doctors, make appointments, review medical
28 treatments and to review charts from previous exams.

1 197. While using Defendant's Web Properties, Plaintiff C.R.T. communicated
2 sensitive—and what she expected to be confidential—personal and medical
3 information to Defendant.

4 198. Plaintiff C.R.T. used AltaMed's Web Properties to research healthcare
5 providers, research particular medical concerns and treatments, fill out forms and
6 questionnaires, schedule and attend appointments and perform other tasks related to
7 her specific medical inquiries and treatment.

8 199. While using AltaMed's Web Properties, Plaintiff C.R.T. communicated
9 and received information regarding her appointments, treatments, medications and
10 clinical information, including lab work. As a result of Defendant choosing to install
11 the Pixel and other tracking technologies on its Web Properties, this information was
12 intercepted, viewed, analyzed and used by unauthorized third parties.

13 200. Plaintiff C.R.T. accessed AltaMed's Web Properties in connection with
14 receiving healthcare services from AltaMed or AltaMed's affiliates at AltaMed's
15 direction and with AltaMed's encouragement.

16 201. Plaintiff C.R.T. has used and continues to use the same devices to
17 maintain and to access an active Facebook account throughout the relevant period.

18 202. Plaintiff C.R.T. noticed that she began receiving targeted advertising on
19 Facebook directed to her medical conditions after researching information regarding
20 that same medical condition on AltaMed's website.

21 203. Specifically, in January 2023, after looking for information about
22 behavioral mental health therapy, she received mental health therapy-related
23 advertisements on Facebook and after searching for a dentist on AltaMed's Web
24 Properties, she began getting dental ads on her Facebook account.

25 204. As a medical patient using AltaMed's health services, Plaintiff C.R.T.
26 reasonably expected that her online communications with AltaMed were solely
27 between herself and AltaMed, and that such communications would not be
28 transmitted or intercepted by a third party. Plaintiff C.R.T. also relied on AltaMed's

1 Privacy Policies in reasonably expecting AltaMed would safeguard her Private
2 Information. But for her status as AltaMed's patient and its representations via its
3 Privacy Policies, Plaintiff C.R.T. would not have disclosed her Private Information to
4 AltaMed.

5 **TOLLING, CONCEALMENT & ESTOPPEL**

6 205. The applicable statutes of limitation have been tolled as a result of
7 Defendant's knowing and active concealment and denial of the facts alleged herein.

8 206. Defendant secretly incorporated the Meta Pixel into its Web Properties
9 and patient portals, providing no indication to Users that their User Data, including
10 their Private Information, would be disclosed to unauthorized third parties.

11 207. Defendant had exclusive knowledge that the Meta Pixel was
12 incorporated on its Web Properties, yet failed to disclose that fact to Users, or
13 inform them that by interacting with its Web Properties, Plaintiffs' and Class
14 Members' User Data, including Private Information, would be disclosed to third
15 parties, including Facebook.

16 208. Plaintiffs and Class Members could not, with due diligence, have
17 discovered the full scope of Defendant's conduct because the incorporation of Meta
18 Pixels is highly technical, and there were no disclosures or other indications that
19 would inform a reasonable consumer that Defendant was disclosing and allowing
20 Facebook to intercept Users' Private Information.

21 209. The earliest Plaintiffs and Class Members could have known about
22 Defendant's conduct was approximately in April or May of 2023. Nevertheless, at
23 all material times herein, Defendant falsely represented to Plaintiffs that their health
24 information is not and will not be disclosed to any third party.

25 210. As alleged above, Defendant has a duty to disclose the nature and
26 significance of its data disclosure practices but failed to do so. Defendant is,
27 therefore, estopped from relying on any statute of limitations under the discovery
28 rule.

CLASS ALLEGATIONS

211. Class Definition: Plaintiffs bring this action on behalf of themselves and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure:

212. The Nationwide Class that Plaintiffs seek to represent is defined as:

Nationwide Class: All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendant's Web Properties.

213. The California Subclass that Plaintiffs seek to represent is defined as:

California Subclass: All individuals residing in the State of California whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendant's Web Properties.

214. The Nationwide Class, and the California Subclass are referred to collectively as the “**Classes**.” Excluded from the Classes are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant’s officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

215. The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors and any entity in which Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel

1 and Defendant's counsel; and (6) the legal representatives, successors and assigns of
2 any such excluded persons.

3 216. Plaintiffs reserve the right under Federal Rule of Civil Procedure 23 to
4 amend or modify the Classes to include a broader scope, greater specificity, further
5 division into subclasses, or limitations to particular issues. Plaintiffs reserve the
6 right under Federal Rule of Civil Procedure 23(c)(4) to seek certification of
7 particular issues.

8 217. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2)
9 and 23(b)(3) are met in this case.

10 218. The Fed. R. Civ. P. 23(a) elements of Numerosity, Commonality,
11 Typicality and Adequacy are all satisfied.

12 219. **Numerosity:** The exact number of Class Members is not available to
13 Plaintiffs, but it is clear that individual joinder is impracticable. Hundreds of
14 thousands of people have used AltaMed's Web Properties since at least 2015.
15 Members of the Class can be identified through Defendant's records or by other
16 means.

17 220. **Commonality:** Commonality requires that the Class Members' claims
18 depend upon a common contention such that determination of its truth or falsity will
19 resolve an issue that is central to the validity of each claim in one stroke. Here, there
20 is a common contention for all Class Members as to whether Defendant disclosed to
21 third parties their Private Information without authorization or lawful authority.

22 221. **Typicality:** Plaintiffs' claims are typical of the claims of other Class
23 Members in that Plaintiffs and the Class Members sustained damages arising out of
24 Defendant's uniform wrongful conduct and data-sharing practices.

25 222. **Adequate Representation:** Plaintiffs will fairly and adequately
26 represent and protect the interests of the Class Members. Plaintiffs' claims are made
27 in a representative capacity on behalf of the Class Members. Plaintiffs have no
28 interests antagonistic to the interests of the other Class Members. Plaintiffs have

1 retained competent counsel to prosecute the case on behalf of Plaintiffs and the
2 Class. Plaintiffs and Plaintiffs' counsel are committed to vigorously prosecuting this
3 action on behalf of the Class members.

4 223. The declaratory and injunctive relief sought in this case includes, but is
5 not limited to:

- 6 a. Entering a declaratory judgment against Defendant—declaring that
7 Defendant's interception of Plaintiffs' and Class Members' Private
8 Information is in violation of the law;
- 9 b. Entering an injunction against Defendant:
 - 10 i. preventing Defendant from sharing Plaintiffs' and Class
11 Members' Private Information among itself and other third
12 parties;
 - 13 ii. requiring Defendant to alert and/or otherwise notify all users of its
14 websites and portals of what information is being collected, used
15 and shared;
 - 16 iii. requiring Defendant to provide clear information regarding its
17 practices concerning data collection from the users/patients of
18 Defendant's Web Properties, as well as uses of such data;
 - 19 iv. requiring Defendant to establish protocols intended to remove all
20 personal information which has been leaked to Facebook and/or
21 other third parties, and request Facebook/third parties to remove
22 such information and
 - 23 v. requiring Defendant to provide an opt out procedure for
24 individuals who do not wish for their information to be tracked
25 while interacting with Defendant's Web Properties.

26 224. **Predominance:** There are many questions of law and fact common to
27 the claims of Plaintiffs and Class Members, and those questions predominate over
28

any questions that may affect individual Class Members. Common questions and/or issues for Class members include, but are not necessarily limited to the following:

- a. Whether Defendant's acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;
- b. Whether Defendant's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
- c. Whether Defendant's acts and practices violated the California Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, *et seq.*;
- d. Whether Defendant's acts and practices violated the California Consumers Legal Remedies Act, Cal. Civ. Code Section 1750 *et seq.*;
- e. Whether Defendant's unauthorized disclosure of Users' Private Information was negligent;
- f. Whether Defendant owed a duty to Plaintiffs' and Class Members not to disclose their Private Information to unauthorized third parties;
- g. Whether Defendant breached its duty to Plaintiffs and Class Members not to disclose their Private Information to unauthorized third parties;
- h. Whether Defendant represented to Plaintiffs and the Class that it would protect Plaintiff's and the Class Members' Private Information;
- i. Whether Defendant violated Plaintiffs' and Class Members' privacy rights;
- j. Whether Plaintiffs and Class Members are entitled to actual damages, enhanced damages, statutory damages and other monetary remedies provided by equity and law;
- k. Whether injunctive and declaratory relief, restitution, disgorgement and other equitable relief is warranted.

225. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable.

1 The damages suffered by individual Class Members will likely be relatively small,
2 especially given the burden and expense of individual prosecution of the complex
3 litigation necessitated by Defendant's actions. Thus, it would be virtually impossible
4 for the individual Class Members to obtain effective relief from Defendant's
5 misconduct. Even if Class Members could mount such individual litigation, it would
6 still not be preferable to a class action, because individual litigation would increase
7 the delay and expense to all parties due to the complex legal and factual
8 controversies presented in this Complaint. By contrast, a class action presents far
9 fewer management difficulties and provides the benefits of single adjudication,
10 economy of scale and comprehensive supervision by a single Court. Economies of
11 time, effort and expense will be enhanced, and uniformity of decisions ensured.

12 226. Likewise, particular issues under Rule 23(c)(4) are appropriate for
13 certification because such claims present only particular, common issues, the
14 resolution of which would advance the disposition of this matter and the parties'
15 interests therein. Such particular issues include, but are not limited to:

- 16 a. Whether Defendant misrepresented that it would disclose personal
17 information only for limited purposes that did not include purposes of
18 delivering advertisements or collecting data for commercial use or
19 supplementing consumer profiles created by data aggregators and
20 advertisers;
- 21 b. Whether Defendant's privacy policies misrepresented that it collected
22 and shared User information with third-party service providers only for
23 the limited purpose of providing access to its services;
- 24 c. Whether Defendant misrepresented that it had in place contractual and
25 technical protections that limit third-party use of User information and
26 that it would seek User consent prior to sharing Private Information with
27 third parties for purposes other than the provision of its services;

- 1 d. Whether Defendant misrepresented that any information it receives is
- 2 stored under the same guidelines as any health entity that is subject to
- 3 the strict patient data sharing and protection practices set forth in the
- 4 regulations propounded under HIPAA;
- 5 e. Whether Defendant misrepresented that it complied with HIPAA's
- 6 requirements for protecting and handling Users' PHI;
- 7 f. Whether Defendant shared the Private Information that Users provided
- 8 to Defendant with advertising platforms, including Facebook, without
- 9 adequate notification or disclosure, and without Users' consent, in
- 10 violation of health privacy laws and rules and its own privacy policy;
- 11 g. Whether Defendant integrated third-party tracking tools, consisting of
- 12 automated web beacons ("Pixels") in its website that shared Private
- 13 Information and User activities with third parties for unrestricted
- 14 purposes, which included advertising, data analytics, and other
- 15 commercial purposes;
- 16 h. Whether Defendant shared Private Information and activity information
- 17 with Facebook using Facebook's tracking Pixels on its Web Properties
- 18 without Users' consent;
- 19 i. Whether Facebook used the information that Defendant shared with it
- 20 for unrestricted purposes, such as selling targeted advertisements, data
- 21 analytics and other commercial purposes.

22 **COUNT I**

23 **VIOLATION OF THE CONFIDENTIALITY OF MEDICAL**
24 **INFORMATION ACT CAL. CIV. CODE §§ 56, et seq.**

25 *(On behalf of Plaintiffs & the California Subclass)*

26 227. Plaintiffs repeat the allegations contained in the paragraphs above as if
27 fully set forth herein.

1 228. Defendant is subject to the CMIA pursuant to California Civil Code
2 § 56.10 because it is a “provider of health care” as defined by California Civil Code
3 § 56.06(b); it operates hospitals, provides health care, maintains medical
4 information, offers software to consumers designed to maintain medical information
5 for the purposes of communications with doctors, receipt of diagnosis, treatment, or
6 management of medical conditions.

7 229. Section 56.10 states, in pertinent part, that “[n]o provider of health care .
8 . . shall disclose medical information regarding a patient of the provider of health
9 care . . . without first obtaining an authorization . . .”

10 230. Section 56.101 of the CMIA states, in pertinent part, that “[a]ny
11 provider of health care . . . who negligently creates, maintains, preserves, stores,
12 abandons, destroys, or disposes of medical information shall be subject to the
13 remedies and penalties . . .” Cal. Civ. Code §§ 56.10, 56.101.

14 231. Plaintiffs’ and the California Subclass Members’ Private Information
15 constitutes “medical information” under the CMIA because it consists of
16 individually identifiable information in possession of and derived from a provider of
17 healthcare regarding Plaintiffs’ and California Subclass Members’ medical history,
18 test results, mental or physical condition and/or treatment.

19 232. Defendant violated Cal. Civ. Code § 56.10 because it failed to maintain
20 the confidentiality of Users’ medical information, and instead “disclose[d] medical
21 information regarding a patient of the provider of health care or an enrollee or
22 subscriber of a health care service plan without first obtaining an authorization” by
23 soliciting, intercepting and receiving Plaintiffs’ and California Subclass Members’
24 Private Information, and sharing it with advertisers and for advertising purposes.
25 Specifically, Defendant knowingly, willfully, or negligently disclosed Plaintiffs’
26 and California Subclass Members’ medical information to Facebook, allowing
27 Facebook to now advertise and target Plaintiffs and California Subclass Members,
28 misusing their extremely sensitive Private Information.

1 233. Defendant violated Cal. Civ. Code § 56.101 because they knowingly,
2 willfully, or negligently failed to create, maintain, preserve, store, abandon, destroy
3 and dispose of medical information in a manner that preserved its confidentiality by
4 soliciting, intercepting, and receiving Plaintiffs' and California Subclass Members'
5 Private Information, and sharing it with advertisers and for advertising purposes for
6 Facebook's and Defendant's financial gain.

7 234. Defendant intentionally embedded Meta Pixels, which facilitate the
8 unauthorized sharing of Plaintiffs' and California Subclass Members' medical
9 information.

10 235. Defendant violated Cal Civ. Code § 56.36(b) because they negligently
11 released confidential information and records concerning Plaintiffs and California
12 Subclass Members in violation of their rights under the CMIA.

13 236. As a direct and proximate result of Defendant's misconduct, Plaintiffs
14 and California Subclass Members had their private communications containing
15 information related to their sensitive and confidential Private Information
16 intercepted, disclosed and used by third parties.

17 237. As a result of Defendant's unlawful conduct, Plaintiffs and California
18 Subclass Members suffered an injury, including violation to their rights of privacy,
19 loss of the privacy of their Private Information, loss of control over their sensitive
20 personal information, and suffered aggravation, inconvenience and emotional
21 distress.

22 238. Plaintiffs and California Subclass Members are entitled to: (a) nominal
23 damages of \$1,000 per violation; (b) actual damages, in an amount to be determined
24 at trial; (c) reasonable attorneys' fees and costs.

25
26
27
28

COUNT II

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY (“CIPA”),
CAL. PENAL CODE § 630, *et seq.*

(On behalf of Plaintiffs & the California Subclass)

239. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

240. Defendant is a person for purposes of Cal. Penal Code §631.

^{241.} CIPA § 631(a) imposes liability for “distinct and mutually independent patterns of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978).

10 Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that
11 defendant, “by means of any machine, instrument, contrivance, or in any other
12 manner,” does any of the following: (1) “intentionally taps, or makes any
13 unauthorized connection...with any telegraph or telephone wire, line, cable, or
14 instrument, including the wire, line, cable, or instrument of any internal telephonic
15 communication system,” (2) “willfully and without the consent of all parties to the
16 communication, or in any unauthorized manner, reads or attempts to read or learn
17 the contents or meaning of any message, report, or communication while the same is
18 in transit or passing over any wire, line or cable or is being sent from or received at
19 any place within [the state of California],” (3) “uses, or attempts to use, in any
20 manner, or for any purpose, or to communicate in any way, any information so
21 obtained,” or (4) *aids, agrees with, employs, or conspires with any person or*
persons to unlawfully do, or permit, or cause to be done any of the acts or things
mentioned above in this section” (emphasis added).

24 242. Section 631(a) is not limited to phone lines, but also applies to “new
25 technologies” such as computers, the Internet and email. *See Matera v. Google Inc.*,
26 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new
27 technologies” and must be construed broadly to effectuate its remedial purpose of
28 protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal.

1 Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook, Inc.*
 2 *Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of
 3 CIPA and common law privacy claims based on Facebook’s collection of
 4 consumers’ Internet browsing history).

5 243. Defendant’s Web Properties are a “machine, instrument, contrivance, or
 6 ... other manner” used to engage in the prohibited conduct at issue here.

7 244. At all relevant times, Defendant entered into contracts with Facebook, in
 8 order to track certain activities on its Web Properties. Defendant allowed Facebook
 9 to intercept and otherwise track Users’ clicks, communications, searches and other
 10 User activities. Defendant activated Meta Pixel tracking tools, allowing Facebook to
 11 intentionally tap, and make unauthorized connections with, the lines of internet
 12 communication between Plaintiffs and California Subclass Members on the one
 13 hand, and Defendant’s Web Properties on the other hand, without consent of all
 14 parties to the communication.

15 245. At all relevant times, by using the Meta Pixel, Facebook willfully and
 16 without the consent of Plaintiffs and California Subclass Members, read or
 17 attempted to learn the contents or meaning of electronic communications of
 18 Plaintiffs and putative California Subclass Members on Defendant’s Web
 19 Properties. This occurred while the electronic communications were in transit or
 20 passing over any wire, line or cable, or were being sent from or received at any
 21 place within California. Facebook intercepted Plaintiffs’ and California Subclass
 22 Members’ communications—including the very terms and phrases they typed into
 23 the search bar—without their authorization or consent.

24 246. Defendant knowingly installed Pixel tracking technology on its Web
 25 Properties, which systematically transmitted all communications between Plaintiffs
 26 and Defendant’s Web Properties to Meta. Indeed, Meta released an explicit
 27 statement to the Court on November 9, 2022, that it neither desired nor intended to
 28 possess health information data. In April 2018, Meta proactively added a clause to

1 its user contract specifying that it requires each of its partners, including Defendant,
 2 to have “lawful” rights to collect, use and share user data before providing any data
 3 to Meta.

4 247. Defendant had the explicit option to disable the Pixel technology on its
 5 Web Properties, but chose not to exercise this option, thereby continuing to share
 6 data with Facebook despite the availability of preventive measures.

7 248. These assertions highlight that Meta advised third-party entities, like
 8 Defendant, to refrain from sending any information they did not have the legal right
 9 to send and expressly emphasized not to transmit health information. Yet,
 10 Defendant, in direct contravention of these advisories and in a clear display of
 11 intent, continued to employ Pixel tracking on its Web Properties, thereby sharing
 12 sensitive patient data without proper authorization or consent.

13 249. Additionally, by embedding Meta Pixels on its Web Properties,
 14 Defendant aided, agreed with, employed and conspired with Facebook to wiretap
 15 consumers communications on Defendant’s Web Properties using the Meta Pixel
 16 snipped codes and to accomplish the wrongful conduct at issue here.

17 250. Plaintiffs and California Subclass Members did not consent to the
 18 interception, reading, learning, recording and collection of their electronic
 19 communications with Defendant. Accordingly, the interception was unlawful and
 20 tortious.

21 251. Defendant both intercepted and aided Facebook in the interception of
 22 “contents” of Plaintiffs’ communications in at least the following forms:

- 23 a. The parties to the communications;
- 24 b. The precise text of patient search queries;
- 25 c. Personally identifying information such as patients’ IP addresses,
 Facebook IDs, browser fingerprints and other unique identifiers;
- 26 d. The precise text of patient communications about specific doctors;
- 27 e. The precise text of patient communications about specific medical

- 1 conditions;
- 2 f. The precise text of information generated when patients requested or
3 made appointments;
- 4 g. The precise text of patient communications about specific treatments;
- 5 h. The precise text of patient communications about scheduling
6 appointments with medical providers;
- 7 i. The precise text of patient communications about billing and payment;
- 8 j. The precise text of specific buttons on Defendant's Webs Properties that
9 patients click to exchange communications, including Log-Ins,
10 Registrations, Requests for Appointments, Search and other buttons;
- 11 k. The precise dates and times when patients click to Log-In on
12 Defendant's Web Properties;
- 13 l. The precise dates and times when patients visit Defendant's Web
14 Properties;
- 15 m. Information that is a general summary or informs third parties of the
16 general subject of communications that Defendant sends back to patients
17 in response to search queries and requests for information about specific
18 doctors, conditions, treatments, billing, payment and other information;
19 and
- 20 n. Any other content that Defendant has aided third parties in scraping
21 from webpages or communication forms at Web Properties.

22 252. Defendant gave substantial assistance to Facebook in violating the
23 privacy rights of Defendant's patients, despite the fact that Defendant's conduct
24 constituted a breach of the duties of confidentiality that medical providers owe their
25 patients. Defendant knew that the installation of the Meta Pixel on its Web
26 Properties would result in the unauthorized disclosure of its patients'
27 communications to Facebook, yet nevertheless did so anyway.

1 253. The violation of section 631(a) constitutes an invasion of privacy
2 sufficient to confer Article III standing.

3 254. Unless enjoined, Defendant will continue to commit the illegal acts
4 alleged here. Plaintiffs continue to be at risk because they frequently use
5 Defendant's Web Properties to search for information about medical products,
6 health conditions or services. Plaintiffs continue to desire to use Defendant's Web
7 Properties for that purpose, including but not limited to investigating health
8 conditions (e.g., diabetes), diagnoses (e.g., COVID-19), procedures, test results,
9 treatment status, the treating physician, medications and/or allergies.

10 255. Plaintiffs and California Subclass Members may or are likely to visit
11 Defendant's Web Properties in the future but have no practical way of knowing
12 whether their website communications will be collected, viewed, accessed, stored
13 and used by Facebook.

14 256. Plaintiffs and California Subclass Members seek all relief available
15 under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of
16 \$5,000 per violation.

17 257. In addition to statutory damages, Defendant's breach caused Plaintiffs
18 and California Subclass Members, at minimum, the following damages:

19 (1) Sensitive and confidential information that Plaintiffs and California Subclass
20 Members intended to remain private is no longer private; and (2) Defendant took
21 something of value from Plaintiffs and California Subclass Members and derived
22 benefit therefrom without Plaintiffs' and California Subclass Members' knowledge
23 or informed consent and without sharing the benefit of such value.

24
25
26
27
28

COUNT III

VIOLATION OF THE UNFAIR COMPETITION LAW (“UCL”)

CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200, et seq.

(On behalf of Plaintiffs & the California Subclass)

258. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

A. Unlawful Prong

259. Defendant's conduct, as alleged herein, was unfair within the meaning of the UCL. The unfair prong of the UCL prohibits unfair business practices that either offend an established public policy or that are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.

260. Defendant's conduct was also fraudulent within the meaning of the UCL. Defendant made deceptive misrepresentations and omitted known material facts in connection with the solicitation, interception, disclosure and use of Plaintiffs' and California Subclass Members' Private Information. Defendant actively concealed and continued to assert misleading statements regarding its protection and limitation on the use of the Private Information. Meanwhile, Defendant was collecting and sharing Plaintiffs' and California Subclass Members' Private Information without their authorization or knowledge to profit off of the information and deliver targeted advertisements to Plaintiffs and California Subclass Members, among other unlawful purposes.

261. Defendant's conduct was further unlawful within the meaning of the UCL because it violated regulations and laws as discussed herein, including but not limited to HIPAA, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq.*

262. Had Plaintiffs and California Subclass Members known Defendant would disclose and misuse their Private Information in contravention of Defendant's

1 representations, they would never have used Defendant's Web Properties Portal and
2 would not have shared their Private Information.

3 263. Defendant's unlawful actions in violation of the UCL have caused and
4 are likely to cause substantial injury to consumers that consumers cannot reasonably
5 avoid themselves, and that is not outweighed by countervailing benefits to
6 consumers or competition.

7 264. As a direct and proximate result of Defendant's misconduct, Plaintiffs
8 and California Subclass Members had their private communications containing
9 information related to their sensitive and confidential Private Information
10 intercepted, disclosed and used by third parties, including but not limited to
11 Facebook.

12 265. As a result of Defendant's unlawful conduct, Plaintiffs and California
13 Subclass Members suffered an injury, including violation of their rights of privacy,
14 loss of value and privacy of their Private Information, loss of control over their
15 sensitive personal information, and suffered embarrassment and emotional distress
16 as a result of this unauthorized sharing of information.

17 **B. Unfair Prong**

18 266. Defendant engaged in unfair business practices by disclosing Plaintiffs'
19 and California Subclass Members' Private Information to unrelated third parties,
20 including Facebook, without prior consent despite its promises to keep such
21 information confidential.

22 267. Defendant's unfair business practices included widespread violations of
23 Plaintiffs' and California Subclass Members' rights to privacy, including its failure
24 to inform the public that using its Web Properties would result in disclosure of
25 highly private information to third parties.

26 268. Because Defendant is in the business of providing medical healthcare
27 services, Plaintiffs and California Subclass Members relied on Defendant to advise
28 them of any potential disclosure of their Private Information.

1 269. Plaintiffs and California Subclass Members were entitled to assume, and
2 did assume, that Defendant would take appropriate measures to keep their Private
3 Information secure and confidential. At no point did Plaintiffs expect to become a
4 commodity on which Defendant and Facebook would trade.

5 270. Plaintiffs and California Subclass Members reasonably relied upon the
6 representations Defendant made in its Privacy Policy, including those
7 representations concerning the confidentiality of Private Information, such as patient
8 health information.

9 271. Defendant was in sole possession of and had a duty to disclose the
10 material information that Plaintiffs' and California Subclass Members' private
11 information was being shared with third parties.

12 272. Had Defendant disclosed that it shared Private Information with third
13 parties, Plaintiffs and the California Subclass Members would not have used
14 Defendant's services at the level they did.

15 273. The harm caused by Defendant's conduct outweighs any potential
16 benefits attributable to such conduct, and there were reasonably available
17 alternatives to further Defendant's legitimate business interests other than
18 Defendant's conduct described herein.

19 274. Defendant's acts, omissions and conduct also violate the unfair prong of
20 the UCL because those acts, omissions and conduct offended public policy
21 (including the aforementioned federal and state privacy statutes and state consumer
22 protection statutes, such as HIPAA), and constitute immoral, unethical, oppressive
23 and unscrupulous activities that caused substantial injury, including to Plaintiffs and
24 California Subclass Members.

25 275. As a direct result of Plaintiffs' and California Subclass Members'
26 reliance on Defendant's representations that Defendant would keep their Private
27 Information confidential and Defendant's express representation that they would not
28 share Private Information with third parties without the Users' express consent,

1 Plaintiffs and California Subclass Members shared highly sensitive information
2 through their use of the Web Properties, causing them to suffer damages when
3 Defendant disclosed said information to a third party.

4 276. As a direct result of Defendant's violations of the UCL, Plaintiffs and
5 California Subclass Members have suffered injury in fact and lost money or
6 property, including but not limited to payments to Defendant and/or other valuable
7 consideration. The unauthorized access to Plaintiffs' and California Subclass
8 Members' private and personal data also diminished the value of that Private
9 Information.

10 277. As a direct result of its unfair practices, Defendant has been unjustly
11 enriched and should be required to make restitution to Plaintiffs and California
12 Subclass Members pursuant to §§ 17203 and 17204 of the California Business &
13 Professions Code, disgorgement of all profits accruing to Defendant because of its
14 unlawful business practices, declaratory relief, attorney's fees and costs (pursuant to
15 Cal. Code Civ. Proc. §1021.5) and injunctive or other equitable relief.

16 **COUNT IV**

17 **INVASION OF PRIVACY—INTRUSION UPON SECLUSION**

18 *(On behalf of Plaintiffs & the Classes)*

19 278. Plaintiffs repeat the allegations contained in the paragraphs above as if
20 fully set forth herein.

21 279. Plaintiffs and Class Members had a reasonable and legitimate
22 expectation of privacy in the Private Information that Defendant failed to adequately
23 protect against disclosure from unauthorized parties.

24 280. Defendant owed a duty to Plaintiffs and Class Members to keep their
25 Private Information confidential.

26 281. Defendant failed to protect and release to unknown and unauthorized
27 third parties the Private Information of Plaintiffs and Class Members.

1 282. By failing to keep Plaintiffs' and Class Members' Private Information
 2 confidential and safe from misuse, Defendant knowingly shared highly sensitive
 3 Private Information with Facebook, Defendant unlawfully invaded Plaintiffs' and
 4 Class Members' privacy by, among others: (i) intruding into Plaintiffs' and Class
 5 Members' private affairs in a manner that would be highly offensive to a reasonable
 6 person; (ii) failing to adequately secure their Private Information from disclosure to
 7 unauthorized persons; and (iii) enabling and facilitating the disclosure of Plaintiffs'
 8 and Class Members' Private Information without authorization or consent.

9 283. Plaintiffs' and Class Members' expectation of privacy was and is
 10 especially heightened given Defendant's consistent representations that Users'
 11 information would remain confidential and would not be disclosed to anyone
 12 without User consent.

13 284. Defendant's privacy policy specifically provides, "AltaMed will only
 14 use or share your health information if it is needed to provide you with health
 15 services."⁶³

16 285. Defendant knew, or acted with reckless disregard, of the fact that a
 17 reasonable person in Plaintiffs' and Class Members' position would consider its
 18 actions highly offensive.

19 286. Defendant's unauthorized surreptitious recording, monitoring and
 20 sharing of the Users' activities, research of diagnosis and treatment and searches for
 21 doctors and medical specialists violated expectations of privacy that have been
 22 established by social norms.

23 287. As a proximate result of such unauthorized disclosures, Plaintiffs' and
 24 Class Members' reasonable expectations of privacy in their Private Information
 25 were unduly frustrated and thwarted and caused damages to Plaintiffs and Class
 26 Members.

27
 28⁶³ See AltaMed Privacy Policy, *supra* note 5.

288. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful and intentional nature of Defendant's conduct, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights.

289. Plaintiffs seek injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and Class Members. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT V
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs & the Classes)

290. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

291. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for services, they entered into implied contracts by which Defendant agreed to safeguard and not disclose such Private Information without consent.

292. Plaintiffs and Class Members accepted Defendant's offers of services and provided their Private Information to Defendant via the Web Properties.

293. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them that included Defendant's promise not to disclose Private Information without consent.

294. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

295. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to third parties, including Facebook.

296. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their Private Information would be disclosed.

297. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT VI

VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT.

CAL. CIV. CODE § 1750, *et seq.* (“CLRA”)

(On behalf of Plaintiffs & the California Subclass)

298. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

299. Defendant engaged in “unfair methods of competition and unfair or deceptive acts . . . in a transaction . . . that result[ed] . . . in the sale . . . of goods” to Plaintiffs and California Subclass Members in violation of Cal. Civ. Code § 1750 and Cal. Civ. Code § 1770(a)(5), (7), (9), (14), (16).

300. For instance, Defendant made representations that it would protect Plaintiffs' and the California Subclass Members' privacy interest, including promising that it will keep Private Information private and secure, that Defendant does not sell Users' Private Information, and that it will only disclose Private Information under certain circumstances, none of which was true.

301. Defendant made these representations with no intention of living up to these representations. Contrary to these representations, Defendant disclosed and allowed third parties to intercept its customers' Private Information.

302. Further, Defendant failed to disclose it secretly shared, used and allowed third parties to intercept Plaintiffs' and California Subclass Members' Private Information.

303. Defendant was under a duty to disclose this information given Defendant's relationship with its customers and Defendant's exclusive knowledge of its misconduct (e.g., the tracking technology incorporated on Defendant's Website, the fact that Private Information is disclosed to unauthorized third parties, that Defendant allowed third parties to intercept Private Information through this technology, and how Defendant and third parties used this data).

304. Plaintiffs and California Subclass Members would not have purchased, or would have paid significantly less for, Defendant's medical services had Defendant not made these false representations. Defendant profited directly from these sales, including through payment for these services, and from the Private Information disclosed and intercepted.

305. Plaintiffs, individually and on behalf of the California Subclass Members, seek an injunction requiring Defendant to obtain consent prior to disclosing and otherwise using Plaintiffs' and California Subclass Members' Private Information and to delete the Private Information already collected, and any other relief which the court deems proper.

COUNT VII

NEGLIGENCE

(On behalf of Plaintiffs & the Classes)

306. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

307. Defendant owed a duty to Plaintiffs and the Class Members to exercise due care in collecting, storing, safeguarding and preventing any disclosure of their Private Information. This duty included but was not limited to: (a) preventing Plaintiffs' and Class Members' Private Information from being to be disclosed to

1 unauthorized third parties; and (b) destroying Plaintiffs' and Class Members'
2 Private Information within an appropriate amount of time after it was no longer
3 required by Defendant.

4 308. Defendant's duties to use reasonable care arose from several sources,
5 including those described below. Defendant had a common law duty to prevent
6 foreseeable harm to others, including Plaintiffs and Class Members, who were the
7 foreseeable and probable victims of any data misuse, such as disclosure of Private
8 Information to unauthorized parties.

9 309. Defendant had a special relationship with Plaintiffs and Class Members,
10 which is recognized by laws and regulations including but not limited to HIPAA, as
11 well as common law. Defendant was in a position to ensure that its systems were
12 sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class
13 Members resulting from unauthorized disclosure of their Private Information to
14 third parties such as Facebook. Plaintiffs and Class Members were compelled to
15 entrust Defendant with their Private Information. At relevant times, Plaintiffs and
16 Class Members understood that Defendant would take adequate data storage
17 practices to safely store their Private Information. Only Defendant could protect
18 Plaintiffs' and Class Members' Private Information collected and stored on
19 Defendant's Web Properties.

20 310. Defendant's duty to use reasonable measures under HIPAA required
21 Defendant to "reasonably protect" confidential data from "any intentional or
22 unintentional use or disclosure" and to "have in place appropriate administrative,
23 technical, and physical safeguards to protect the privacy of [PHI]." 45 C.F.R.
24 § 164.530(c)(1).

25 311. Defendant's conduct, as described above, constituted an unlawful
26 breach of its duty to exercise due care in collecting, storing and safeguarding
27 Plaintiffs' and the Class Members' Private Information by failing to protect this
28 information.

1 312. Defendant breached its duty in this relationship to collect and safely
2 store Plaintiffs' and Class Members' Private Information.

3 313. Plaintiffs' and the Class Members' Private Information would have
4 remained private and secure had it not been for Defendant's wrongful and negligent
5 breach of its duties. Defendant's negligence was, at least, a substantial factor in
6 causing Plaintiffs' and Class Members' Private Information to be improperly
7 accessed, disclosed and otherwise compromised, and in causing Plaintiffs and the
8 Class Members other injuries because of the unauthorized disclosures.

9 314. The damages suffered by Plaintiffs and the Class Members were the
10 direct and reasonably foreseeable result of Defendant's negligent breach of its duties
11 to maintain Users' Private Information. Defendant knew or should have known that
12 its unauthorized disclosure of highly sensitive Private Information was a breach of
13 its duty to collect and safely store such information.

14 315. Defendant's negligence directly caused significant harm to Plaintiffs
15 and the Class. Specifically, Plaintiffs and Class Members are now subject to their
16 sensitive information being accessed by unauthorized parties, which may lead to
17 significant harm.

18 316. Plaintiffs hereby incorporate all other paragraphs as if fully stated
19 herein.

20 317. Defendant had a fiduciary duty to protect the confidentiality of its
21 communications with Plaintiffs and Class Members by virtue of the explicit privacy
22 representations Defendant made on its Websites to Plaintiffs and members of the
23 Class.

24 318. Defendant had information relating to Plaintiffs and Class Members that
25 it knew or should have known to be confidential.

26 319. Plaintiffs' and Class Members' communications with Defendant about
27 sensitive Private Information and their status as patients of Defendant were not
28 matters of general knowledge.

320. Defendant breached its fiduciary duty of confidentiality by designing its data protection systems in a way that allows for a data breach of a massive caliber.

321. At no time did Plaintiffs or Class Members give informed consent to Defendant's conduct.

322. As a direct and proximate cause of Defendant's actions, Plaintiffs and Class Members suffered damage in that the information they intended to remain private is no longer so and their Private Information was disclosed to, tracked and intercepted by third-party Internet tracking companies, including Facebook, without their knowledge or consent.

COUNT VIII
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs & the Classes)

323. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

324. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

325. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

326. Plaintiffs' and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Privacy Policies.

327. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel (and other tracking technologies) to disclose and transmit Plaintiffs' and Class Members' Private Information and the contents of their communications exchanged with Defendant to third parties.

328. The third-party recipients included, but were not limited to, Facebook and other online marketers.

1 329. Defendant's disclosures of Plaintiffs' and Class Members' Private
2 Information were made without their knowledge, consent or authorization, and were
3 unprivileged.

4 330. The harm arising from a breach of provider-patient confidentiality
5 includes erosion of the essential confidential relationship between the healthcare
6 provider and the patient.

7 331. As a direct and proximate cause of Defendant's unauthorized
8 disclosures of patient personally identifiable, non-public medical information, and
9 communications, Plaintiffs and Class Members were damaged by Defendant's
10 breach in that:

- 11 a. Sensitive and confidential information that Plaintiffs and Class
12 Members intended to remain private is no longer private;
- 13 b. Defendant eroded the essential confidential nature of the provider-
14 patient relationship;
- 15 c. Defendant took something of value from Plaintiffs and Class Members
16 and derived benefit therefrom without Plaintiffs' and Class Members'
17 knowledge or informed consent and without compensating Plaintiffs and
18 Class Members for the data;
- 19 d. Plaintiffs and Class Members did not get the full value of the medical
20 services for which they paid, which included Defendant's duty to
21 maintain confidentiality;
- 22 e. Defendant's actions diminished the value of Plaintiffs' and Class
23 Members' Private Information; and
- 24 f. Defendant's actions violated the property rights Plaintiffs and Class
25 Members have in their Private Information.

26 332. Plaintiffs and Class Members are, therefore, entitled to general damages
27 for invasion of their rights in an amount to be determined by a jury and nominal
28

1 damages for each independent violation. Plaintiffs are also entitled to punitive
2 damages.

3 **COUNT IX**

4 **BREACH OF FIDUCIARY DUTY**

5 ***(On Behalf of Plaintiffs & the Classes)***

6 333. Plaintiffs repeat the allegations contained in the paragraphs above as if
7 fully set forth herein.

8 334. In light of the special relationship between Defendant and Plaintiffs and
9 Class Members, whereby Defendant became guardian of Plaintiffs' and Class
10 Members' Private Information, Defendant became a fiduciary by its undertaking
11 and guardianship of the Private Information, to act primarily for Plaintiffs and Class
12 Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private
13 Information; (2) to timely notify Plaintiffs and Class Members of an unauthorized
14 disclosure; and (3) to maintain complete and accurate records of what information
15 (and where) Defendant did and does store.

16 335. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and
17 Class Members upon matters within the scope of Defendant' relationship with its
18 patients and former patients, in particular, to keep secure their Private Information.

19 336. Defendant breached its fiduciary duties to Plaintiffs and Class Members
20 by disclosing their Private Information to unauthorized third parties, and separately,
21 by failing to notify Plaintiffs and Class Members of this fact.

22 337. As a direct and proximate result of Defendant' breach of its fiduciary
23 duties, Plaintiffs and Class Members have suffered and will continue to suffer injury
24 and are entitled to compensatory, nominal, and/or punitive damages, and
25 disgorgement of profits, in an amount to be proven at trial.

COUNT X

UNJUST ENRICHMENT

(On behalf of Plaintiffs & the Classes)

338. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

339. Plaintiffs and Class Members personally and directly conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiffs' and Class Members' Private Information. Defendant was aware of Plaintiffs' privacy expectations, and in fact, promised to maintain Plaintiffs' Private Information confidentially and not to disclose it to third parties. Defendant received payments for medical services from Plaintiffs and Class Members.

340. Plaintiffs and Class Members also conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used and disclosed this information for its own gain, including for advertisement, market research, sale, or trade for valuable benefits from Facebook and other third parties. Defendant had knowledge that Plaintiffs and Class Members had conferred this benefit on Defendant by interacting with its Web Properties, and Defendant intentionally installed the Meta Pixel tool on its Web Properties to capture and monetize this benefit conferred by Plaintiffs and Class Members.

341. Plaintiffs and Class Members would not have used Defendant's Web Properties had they known that Defendant would collect, use and disclose this information to Facebook, Google and other third parties. The services that Plaintiffs and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with

1 Defendant would be treated as confidential and would never be disclosed to third
2 parties for marketing purposes without the express consent of patients.

3 342. The medical services that Defendant offers are available from many
4 other healthcare systems that protect the confidentiality of patient communications.
5 Had Defendant disclosed that it would allow third parties to secretly collect
6 Plaintiffs' and Class Members' Private Health Information without consent, neither
7 Plaintiffs, the Class Members, nor any reasonable person would have purchased
8 healthcare from Defendant and/or its affiliated healthcare providers.

9 343. By virtue of the unlawful, unfair and deceptive conduct alleged herein,
10 Defendant knowingly realized hundreds of millions of dollars in revenue from the
11 use of the Private Information of Plaintiffs and Class Members for profit by way of
12 targeted advertising related to Users' respective medical conditions and treatments
13 sought.

14 344. This Private Information, the value of the Private Information, and/or
15 the attendant revenue were monetary benefits conferred upon Defendant by
16 Plaintiffs and Class Members.

17 345. As a result of Defendant's conduct, Plaintiffs and Class Members
18 suffered actual damages in the loss of value of their Private Information and lost
19 profits from the use of their Private Information.

20 346. It would be inequitable and unjust to permit Defendant to retain the
21 enormous economic benefits (financial and otherwise) it has obtained from and/or at
22 the expense of Plaintiffs and Class Members.

23 347. Defendant will be unjustly enriched if it is permitted to retain the
24 economic benefits conferred upon them by Plaintiffs and Class Members through
25 Defendant's obtaining the Private Information and the value thereof, and profiting
26 from the unlawful, unauthorized and impermissible use of the Private Information of
27 Plaintiffs and Class Members.

348. Plaintiffs and Class Members are, therefore, entitled to recover the amounts realized by Defendant at the expense of Plaintiffs and Class Members.

349. Plaintiffs and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendant's ill-gotten gains and/or other sums as may be just and equitable.

COUNT XI

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT **(“ECPA”)**

18 U.S.C. § 2511(1), et seq.

Unauthorized Interception, Use and Disclosure

(On Behalf of Plaintiffs & the Classes)

350. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

351. The ECPA protects both sending and receipt of communications.

352. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

353. The transmissions of Plaintiffs' PII and PHI to Defendant's Web Properties qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

354. **Electronic Communications.** The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Web Properties with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

1 355. **Content.** The ECPA defines content, when used with respect to
2 electronic communications, to “include[] any information concerning the substance,
3 purport, or meaning of that communication.” 18 U.S.C. § 2510(8) (emphasis
4 added).

5 356. Defendant’s intercepted communications include, but are not limited to,
6 communications to/from Plaintiffs and Class Members regarding PII and PHI,
7 diagnosis of certain conditions, treatment/medication for such conditions, and
8 scheduling of appointments, including annual mammograms, surgeries, emergency
9 room visits, lab work and scans. Furthermore, Defendant intercepted the “contents”
10 of Plaintiffs’ communications in at least the following forms:

- 11 a. The parties to the communications;
- 12 b. The precise text of patient search queries;
- 13 c. Personally, identifying information such as patients’ IP addresses,
14 Facebook IDs, browser fingerprints and other unique identifiers;
- 15 d. The precise text of patient communications about specific doctors;
- 16 e. The precise text of patient communications about specific medical
17 conditions;
- 18 f. The precise text of information generated when patients requested or
19 made appointments,
- 20 g. The precise text of patient communications about specific treatments;
- 21 h. The precise text of patient communications about scheduling
22 appointments with medical providers;
- 23 i. The precise text of patient communications about billing and payment;
- 24 j. The precise text of specific buttons on Defendant’s Web Properties that
25 patients click to exchange communications, including Log-Ins,
26 Registrations, Requests for Appointments, Search and other buttons;
- 27 k. The precise dates and times when patients click to Log-In on
28 Defendant’s Web Properties;

- 1 l. The precise dates and times when patients visit Defendant's Web
2 Properties;
- 3 m. Information that is a general summary or informs third parties of the
4 general subject of communications that Defendant sends back to patients
5 in response to search queries and requests for information about specific
6 doctors, conditions, treatments, billing, payment and other information.

7 357. **Interception**. The ECPA defines the interception as the "acquisition of
8 the contents of any wire, electronic, or oral communication through the use of any
9 electronic, mechanical, or other device" and "contents ... include any information
10 concerning the substance, purport, or meaning of that communication." 18 U.S.C.
11 § 2510(4), (8).

12 358. **Electronical, Mechanical or Other Device**. The ECPA defines
13 "electronic, mechanical, or other device" as "any device ... which can be used to
14 intercept a[n] ... electronic communication[.]" 18 U.S.C. § 2510(5). The following
15 constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

- 16 a. Plaintiffs' and Class Members' browsers;
- 17 b. Plaintiffs' and Class Members' computing devices
- 18 c. Defendant's web servers; and
- 19 d. The Pixel code deployed by Defendant to effectuate the sending and
20 acquisition of patient communications.

21 359. By utilizing and embedding the Pixel on its Web Properties, Defendant
22 intentionally intercepted, endeavored to intercept and procured another person to
23 intercept, the electronic communications of Plaintiffs and Class Members, in
24 violation of 18 U.S.C. § 2511(1)(a).

25 360. Specifically, Defendant intercepted Plaintiffs' and Class Members'
26 electronic communications via the Pixel, which tracked, stored and unlawfully
27 disclosed Plaintiffs' and Class Members' Private Information to third parties such as
28 Facebook.

1 361. Defendant's intercepted communications include, but are not limited to,
2 communications to/from Plaintiffs and Class Members regarding PII and PHI,
3 treatment, medication and scheduling.

4 362. By intentionally disclosing or endeavoring to disclose the electronic
5 communications of Plaintiffs and Class Members to affiliates and other third parties,
6 while knowing or having reason to know that the information was obtained through
7 the interception of an electronic communication in violation of 18 U.S.C. §
8 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

9 363. By intentionally using, or endeavoring to use, the contents of the
10 electronic communications of Plaintiffs and Class Members, while knowing or
11 having reason to know that the information was obtained through the interception of
12 an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant
13 violated 18 U.S.C. § 2511(1)(d).

14 364. **Unauthorized Purpose.** Defendant intentionally intercepted the
15 contents of Plaintiffs' and Class Members' electronic communications for the
16 purpose of committing a tortious act in violation of the Constitution or laws of the
17 United States or of any State—namely, invasion of privacy, among others.

18 365. The ECPA provides that a “party to the communication” may be liable
19 where a “communication is intercepted for the purpose of committing any criminal
20 or tortious act in violation of the Constitution or laws of the United States or of any
21 State.” 18 U.S.C § 2511(2)(d).

22 366. Defendant is not a party for purposes to the communication based on its
23 unauthorized duplication and transmission of communications with Plaintiffs and
24 the Class. However, even assuming Defendant is a party, Defendant's simultaneous,
25 unknown duplication, forwarding and interception of Plaintiffs' and Class
26 Members' Private Information does not qualify for the party exemption.

27 367. Defendant's acquisition of patient communications that were used and
28 disclosed to Facebook was done for purposes of committing criminal and tortious

1 acts in violation of the laws of the United States and individual States nationwide as
2 set forth herein, including:

- 3 a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- 4 b. Invasion of privacy;
- 5 c. Breach of confidence;
- 6 d. Breach of fiduciary duty;
- 7 e. California Invasion of Privacy Act, §§ 630, *et seq.*;
- 8 f. California Confidentiality of Medical Information Act, Cal. Civ. Code
9 §§ 56, *et seq.*;

10 368. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and
11 caused to be used cookie identifiers associated with specific patients without patient
12 authorization; and disclosed individually identifiable health information to
13 Facebook without patient authorization.

14 369. The penalty for violation is enhanced where "the offense is committed
15 with intent to sell, transfer, or use individually identifiable health information for
16 commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

17 370. Defendant's conduct would be subject to the enhanced provisions of
18 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook source code was for
19 Defendant's commercial advantage to increase revenue from existing patients and
20 gain new patients.

21 371. Defendant is not exempt from ECPA liability under 18 U.S.C.
22 § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class
23 Members' communications about their Private Information on its Web Properties,
24 because it used its participation in these communications to improperly share
25 Plaintiffs' and Class Members' Private Information with Facebook and third-parties
26 that did not participate in these communications, that Plaintiffs and Class Members
27 did not know was receiving their information, and that Plaintiffs and Class Members
28 did not consent to receive this information.

372. As such, Defendant cannot viably claim any exception to ECPA liability.

373. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about their medical symptoms, conditions and concerns, medical appointments, healthcare providers and locations, medications and treatments and health insurance and medical bills) for commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;
 - b. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' PII and PHI without providing any value or benefit to Plaintiffs or the Class members;
 - c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and the Class Members' PII and PHI, such as understanding how people use its Web Properties and determining what ads people see on its Web Properties, without providing any value or benefit to Plaintiffs or the Class Members;
 - d. Defendant has failed to provide Plaintiffs and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of its patient information; and
 - e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

374. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' Private Information for financial gain.

375. Defendant was not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communication.

376. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the Pixel.

377. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

378. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Web Properties, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

379. As a result of Defendant's violation of the ECPA, Plaintiffs and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Proposed Class defined herein, respectfully request:

- A. That this Action be maintained as a Class Action, that Plaintiffs be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;
 - B. That the Court enter an order:

- 1 a. Preventing Defendant from sharing Plaintiffs' and Class
2 Members' Private Information among other third parties;
- 3 b. Requiring Defendant to alert and/or otherwise notify all
4 users of its Websites and Portals of what information is
5 being collected, used and shared;
- 6 c. Requiring Defendant to provide clear information regarding
7 its practices concerning data collection from the
8 users/patients of Defendant's Web Properties, as well as uses
9 of such data;
- 10 d. Requiring Defendant to establish protocols intended to
11 remove all personal information which has been leaked to
12 Facebook and/or other third parties, and request
13 Facebook/third parties to remove such information;
- 14 e. Requiring Defendant to provide an opt-out procedure for
15 individuals who do not wish for their information to be
16 tracked while interacting with Defendant's Web Properties;
- 17 f. Mandating the proper notice be sent to all affected
18 individuals and posted publicly;
- 19 g. Requiring Defendant to delete, destroy, and purge the Private
20 Information of Users unless Defendant can provide
21 reasonable justification for the retention and use of such
22 information when weighed against the privacy interests of
23 Users;
- 24 h. Requiring all further and just corrective action, consistent
25 with permissible law and pursuant to only those causes of
26 action so permitted.

27
28

- 1 C. That the Court award Plaintiffs and the Class Members damages (both
2 actual damages for economic and non-economic harm and statutory
3 damages) in an amount to be determined at trial;
- 4 D. That the Court issue appropriate equitable and any other relief
5 (including monetary damages, restitution and/or disgorgement) against
6 Defendant to which Plaintiffs and the Class are entitled, including but
7 not limited to restitution and an Order requiring Defendant to cooperate
8 and financially support civil and/or criminal asset recovery efforts;
- 9 E. Plaintiffs and the Class be awarded with pre- and post-judgment
10 interest (including pursuant to statutory rates of interest set under State
11 law);
- 12 F. Plaintiffs and the Class be awarded reasonable attorneys' fees and costs
13 of suit incurred by their attorneys;
- 14 G. Plaintiffs and the Class be awarded with treble and/or punitive damages
15 insofar as they are allowed by applicable laws; and
- 16 H. Any and all other such relief as the Court may deem just and proper
17 under the circumstances.

18 **JURY TRIAL DEMANDED**

19 Plaintiffs demand a jury trial on all triable issues.

20 DATED: November 14, 2023

21 /s/ Daniel Srourian

22 Daniel Srourian, California Bar No.
23 285678
24 **SROURIAN LAW FIRM, P.C.**
25 3435 Wilshire Blvd. Suite 1710
26 Los Angeles, CA 90010
27 daniel@slfla.com

1 John R. Parker, Jr., California Bar No.
2 257761

3 **ALMEIDA LAW GROUP LLC**
4 3550 Watt Avenue, Suite 140
Sacramento, California 95821
jrparker@almeidalawgroup.com

5 David S. Almeida (*pro hac vice*
6 *forthcoming*)

7 Britany A. Kabakov (*pro hac vice*
forthcoming)

8 Matthew J. Langley, California Bar No.
9 342846

10 **ALMEIDA LAW GROUP LLC**
11 849 W. Webster Avenue
Chicago, Illinois 60614
t: 312-576-3024
david@almeidalawgroup.com
matt@almeidalawgroup.com